42crunch

13 July 2023

Deep dive into API security with 42Crunch and GitHub

Isabelle Mauny

Field CTO and Co-Founder

Colin Domoney

Chief Technology Evangelist

Introduction

About the Speakers

Isabelle Mauny

Field CTO and Co-Founder

WSO2, Axway, Vordel

Colin Domoney

Chief Technology Evangelist

Editor of APISecurity.io
CyberProof, CA, Veracode, Deutsche Bank

Housekeeping Rules

- All attendees muted
- Questions via Q&A
- Recording will be shared
- Polling questions

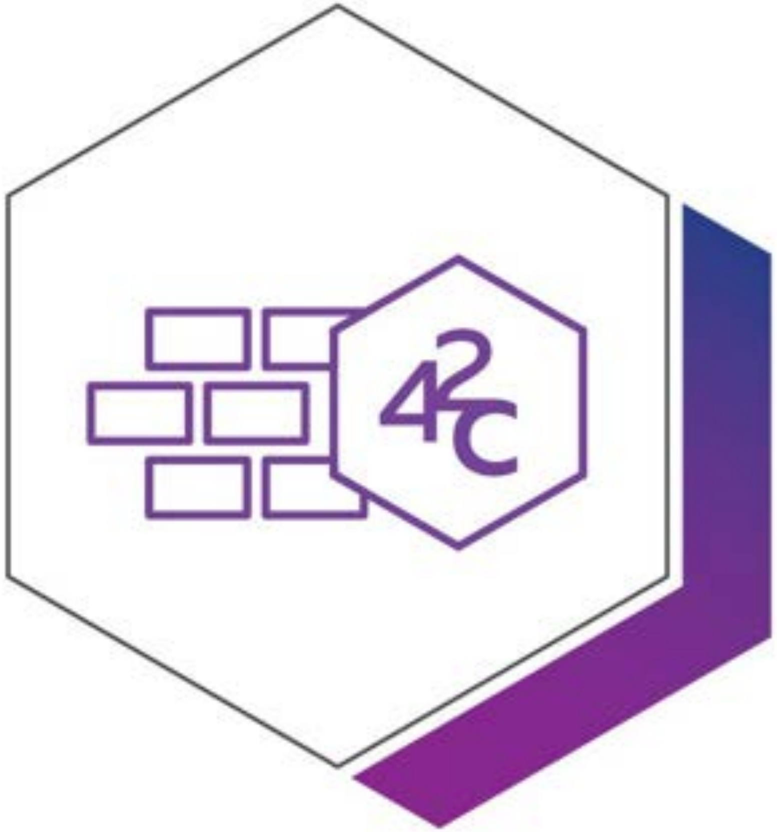
Agenda

- 42Crunch Philosophy
- API Security Testing
- Live demo
  - API Discovery
  - Running API Static and Dynamic Testing
  - Compliance Enforcement
- Questions and Answers

Question One:

How are you **primarily** testing your APIs during design and development?

1. Manual testing with Postman
2. Automated testing with Newman
3. Using unit test frameworks
4. Using SmartBear’s ReadyAPI
5. Command line with curl



Our approach to API security

Shift-Left and Shield-Right

The benefits of Shift-Left for API security

- **Reduced cost** of deployment and rework
- **Reduced risk exposure** due to early elimination of vulnerabilities
- **Improved developer awareness** of security concerns and best practice
- **Secure by design**, rather than by testing

INNOVATION

16 Industry Experts Share Tips For Creating A Security-First Tech Company

Expert Panel® Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

am EDT

When Security Meets Development: The DevSecOps Conundrum

The DevSecOps journey is well worth undertaking be
development, and ensure quality products

Home » Security Boulevard (Original) » The Benefits of Shift Left Security

The Benefits of Shift Left Security

by Lucjan Zaborowski on March 25, 2022

Continuous API Security

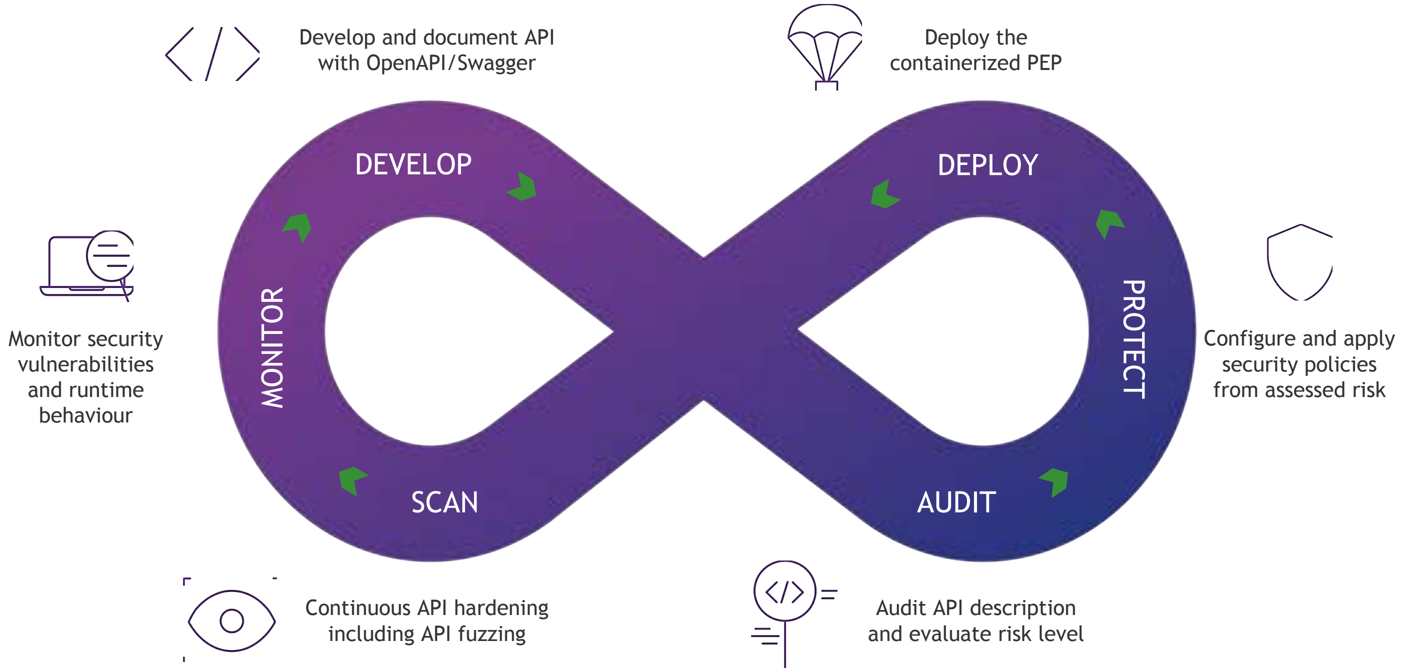
Automate and Scale API Security to Protect Your APIs

SHIFT LEFT

- Growing recognition of need to include security at design time
- ***Security as code** for a seamless DevSecOps experience*
- *Embed and **automate security** in the API development CI/CD pipeline.*

SHIELD RIGHT

- *Security teams retain control and visibility of the **enforcement** of API security policies.*
- ***Low-footprint** containerized PEP enforces all policies at runtime.*



Develop and document API with OpenAPI/Swagger

Deploy the containerized PEP

DEVELOP

DEPLOY

Monitor security vulnerabilities and runtime behaviour

MONITOR

PROTECT

Configure and apply security policies from assessed risk

SCAN

AUDIT

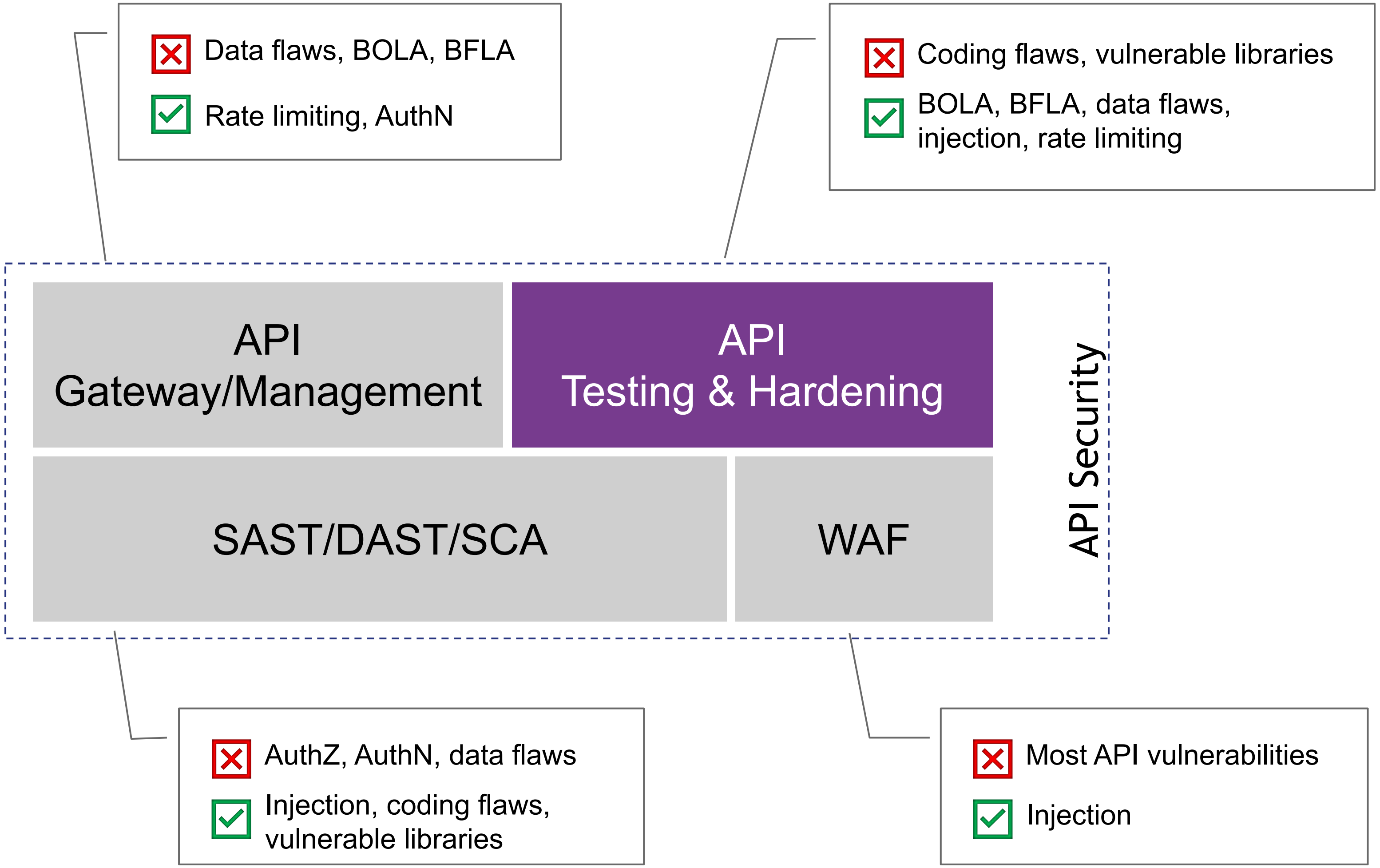
Continuous API hardening including API fuzzing

Audit API description and evaluate risk level

API Security Testing

Defense in depth

Where does API security fit?



☒ Data flaws, BOLA, BFLA

☑ Rate limiting, AuthN

☒ Coding flaws, vulnerable libraries

☑ BOLA, BFLA, data flaws, injection, rate limiting

☒ AuthZ, AuthN, data flaws

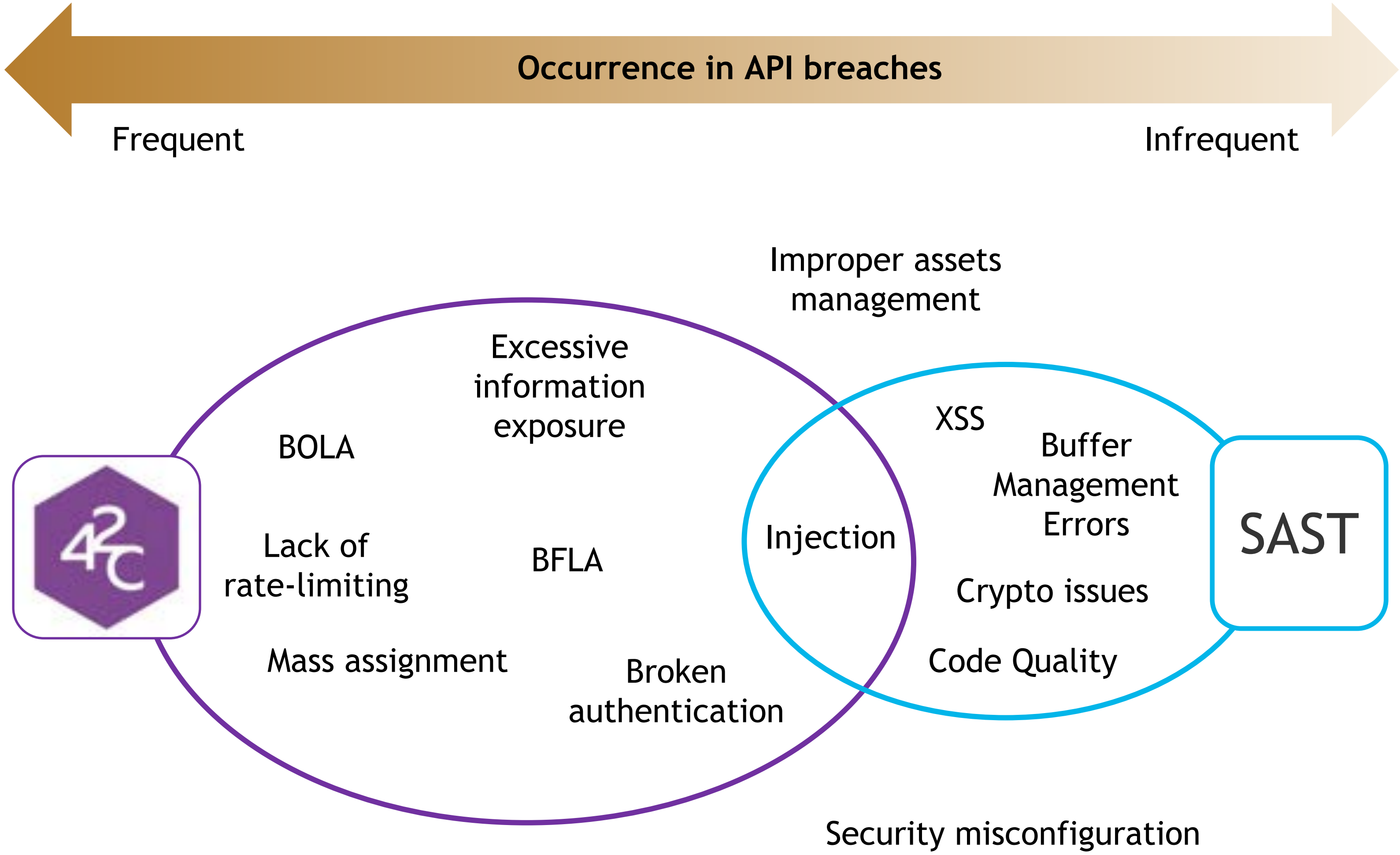
☑ Injection, coding flaws, vulnerable libraries

☒ Most API vulnerabilities

☑ Injection

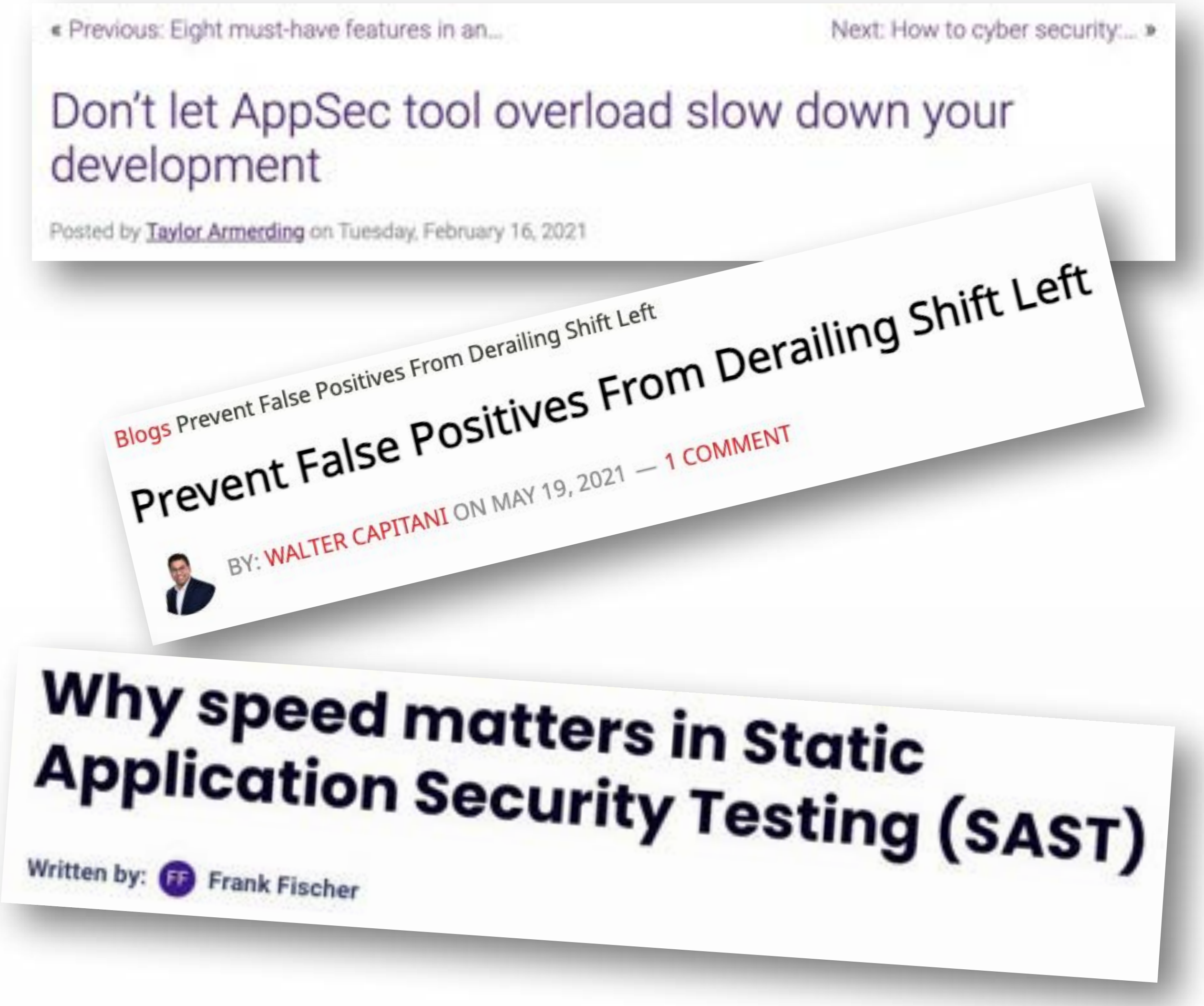
#	OWASP API Top 10 Vulnerabilities
1	Broken Object Level Authorization
2	Broken Authentication
3	Broken Object Property Level Authorization
4	Unrestricted Resource Consumption
5	Broken Function Level Authorization
6	Unrestricted Access to Sensitive Business Flows
7	Server-Side Request Forgery
8	Security Misconfiguration
9	Improper Inventory Management
10	Unsafe Consumption of APIs

SAST versus API Security



Developer frustrations with security testing

- **False positives**
- Findings **received too late** in the lifecycle
- Findings must be viewed in another platform **outside of their usual workflow**
- Findings are **not actionable** – not their own code or change request



« Previous: Eight must-have features in an... Next: How to cyber security:... »

Don't let AppSec tool overload slow down your development

Posted by Taylor Armerding on Tuesday, February 16, 2021

Blogs Prevent False Positives From Derailing Shift Left

Prevent False Positives From Derailing Shift Left

BY: WALTER CAPITANI ON MAY 19, 2021 — 1 COMMENT

Why speed matters in Static Application Security Testing (SAST)

Written by: FF Frank Fischer

Security testing in GitHub

Supply Chain Security

Secure the open-source dependencies your applications rely on, either directly or by inheritance

Secret Scanning

Scans for over 100+ token types, provided by vendors

Extensible with custom patterns for secret detection

Code Scanning

Static analysis of every pull request, integrated into the developer workflow and powered by CodeQL and integrations like 42Crunch

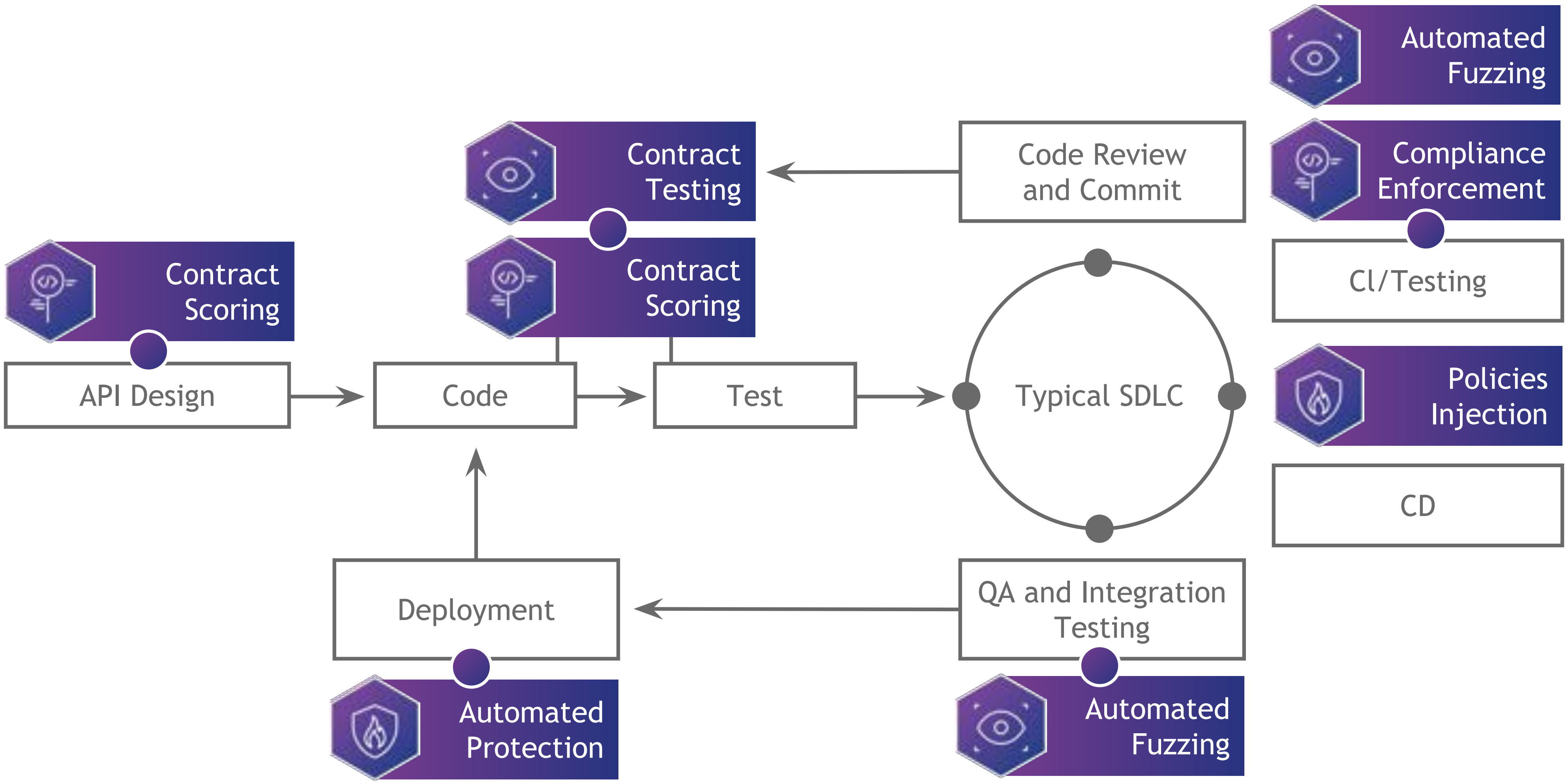
Question Two:

What are you using for static code analysis currently?

1. Github Advanced Security
2. Veracode/Checkmarx, etc
3. Sonarqube
4. Semgrep
5. None

Live demo

How the 42Crunch Platform Works?



Contract Scoring

API Design

Contract Testing

Contract Scoring

Code

Test

Code Review and Commit

Typical SDLC

Deployment

Automated Protection

QA and Integration Testing

Automated Fuzzing

Automated Fuzzing

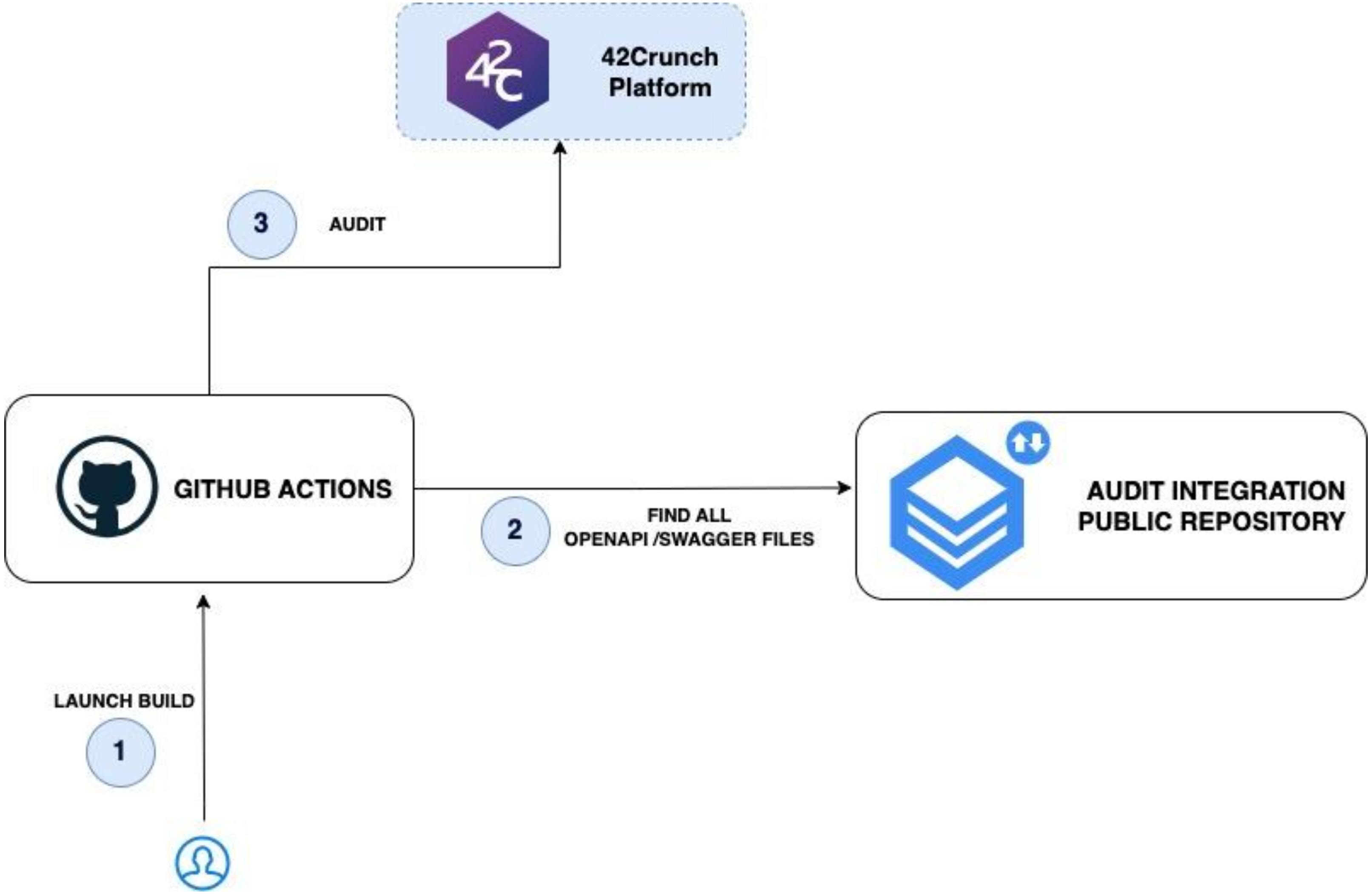
Compliance Enforcement

CI/Testing

Policies Injection

CD

APIs Discovery And Analysis



42Crunch Platform

3 AUDIT

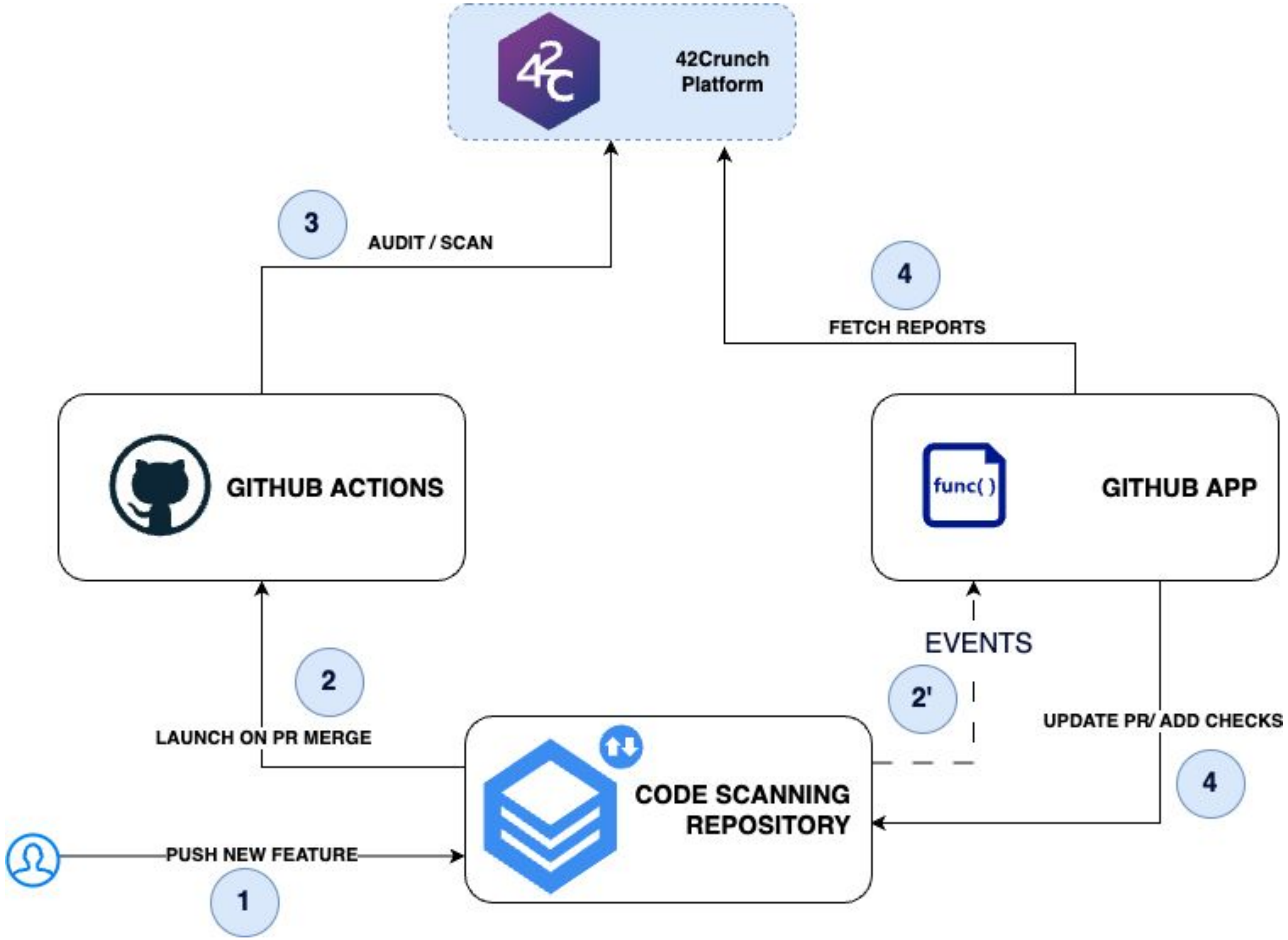
GITHUB ACTIONS

2 FIND ALL OPENAPI /SWAGGER FILES

AUDIT INTEGRATION PUBLIC REPOSITORY

LAUNCH BUILD 1

PR Deployment Flow



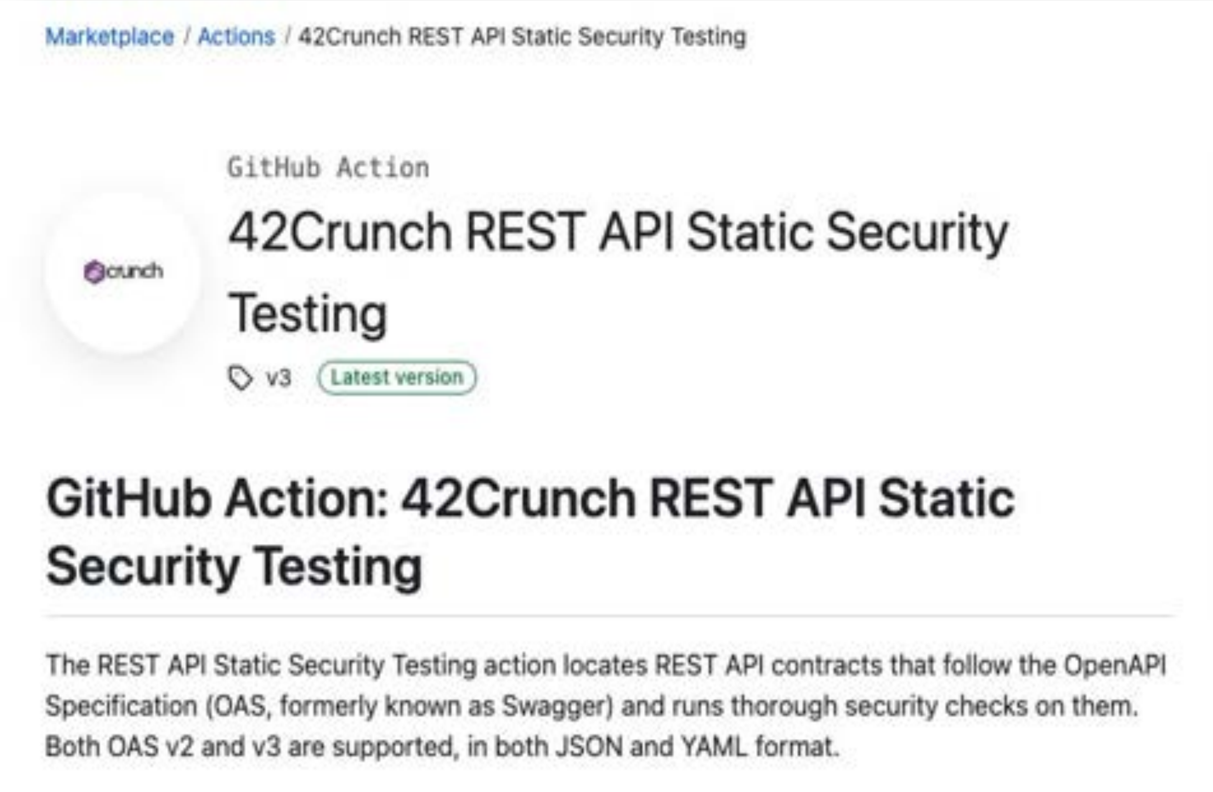
Attendee Question:

How does the “find contracts in repositories” action work? grepping json/yaml files for “openapi”?

Learning more and next steps

How to get started

Using the 42Crunch extensions



Marketplace / Actions / 42Crunch REST API Static Security Testing

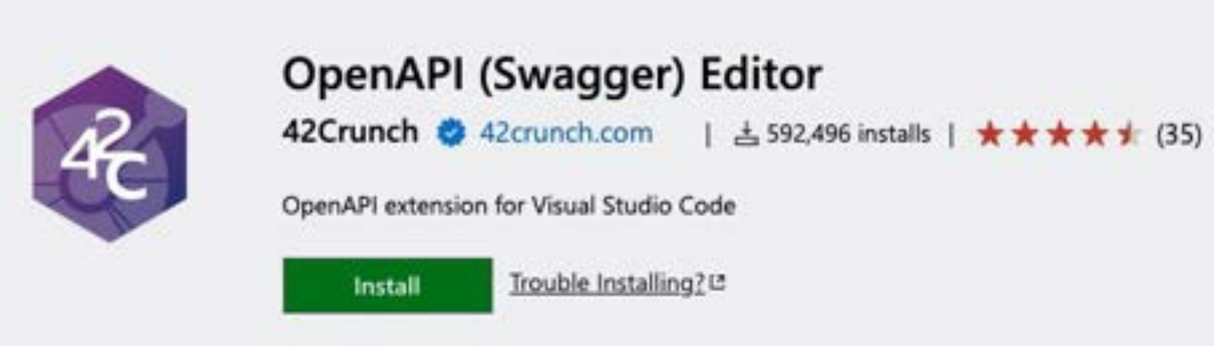
GitHub Action

42Crunch REST API Static Security Testing

v3 Latest version

GitHub Action: 42Crunch REST API Static Security Testing

The REST API Static Security Testing action locates REST API contracts that follow the OpenAPI Specification (OAS, formerly known as Swagger) and runs thorough security checks on them. Both OAS v2 and v3 are supported, in both JSON and YAML format.



OpenAPI (Swagger) Editor

42Crunch 42crunch.com | 592,496 installs | ★★★★★ (35)

OpenAPI extension for Visual Studio Code

https://github.com/marketplace/actions/42crunch-rest-api-static-security-testing

https://marketplace.visualstudio.com/items?itemName=42Crunch.vscode-openapi

Attendee Question:

IntelliJ plugin - does it support the same level

Attendee Question:

The tests are executed locally and on github, right?
How do we ensure the tests are the same. same settings etc? can we push the ‘config’ to all users?

Attendee Question:

Is there a dashboard for security personnel to see an overview of all API security positions?

Attendee Question:

Are there equivalents in gitlab?

Join our next webinar

42crunch

WEBINAR

Something Old, Something New: OWASP API Security Top 10 2023

August 1, 2023 | 9am PDT | 5pm BST

Colin Domoney
Chief Technology Evangelist
42Crunch

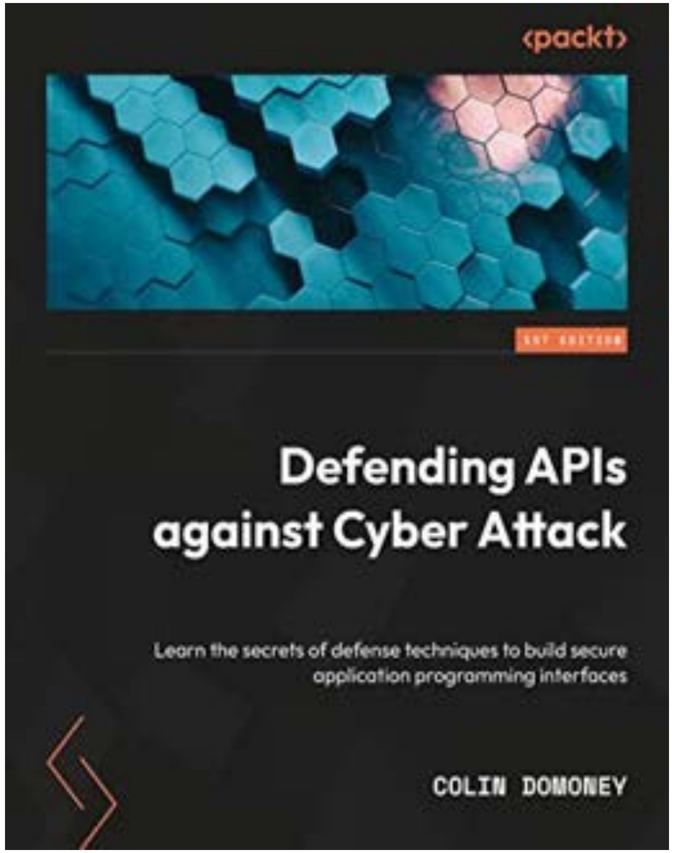
https://42crunch.com/something-old-something-new-owasp-api-security-top-10-2023/

Learning more

#1 API Security Newsletter APISecurity.io

https://apisecurity.io/

“Defending APIs against Cyber Attack” by Colin Domoney


‹packt›
1ST EDITION
Defending APIs against Cyber Attack
Learn the secrets of defense techniques to build secure application programming interfaces
COLIN DOMONEY

https://amzn.to/3fHp8Mz