{ API:WORLD™ }

OCT 24–26 Santa Clara, CA OCT 31–NOV 2 Live Online

API Security: Have we failed to deliver?

Isabelle MAUNY | @isamauny

Field CTO & Co-Founder - 42Crunch

Glad to be here!

- Field CTO / Founder of 42Crunch and apisecurity.io
- French National, I have lived in Spain for the past 20 years
- Most of career in the integration world, pioneering in 2004 what would become API Management
- This presentation and sample code at: https://github.com/isamauny/apiworld-2023

6 years ago…

What has changed ?

Close Your API Security Gaps, Prevent Breaches With These Five Best Practices

By Will Au | September 2, 2023

Adopting these five best practices can help protect companies and minimize the impact of cyberattacks resulting in API security breaches.

Application programming interfaces, or APIs, have been around since the early days of computing, but it's only relatively recently that their popularity has exploded. Now, APIs play a part in 83% of Internet traffic in everyday services like PayPal and Google Maps. And, because APIs facilitate data exchange between different microservices, they also provide access to a trove of sensitive data. Because of that, APIs are an extremely attractive target for security breaches.

In fact, data shows that the number of API breaches is on track to accelerate at a rate of 227% — quite a jump as compared with 2022 (172%) and 2021 (117%). Cybercriminals target APIs through a range of methods:

Faces before interfaces

API Security Needs a Reset—with People, not Tools

Matias Madou
Co-founder & CTO, Secure Code Warrior

It is increasingly challenging for developers and security teams to keep the application-development process and application programming interfaces (APIs) secure. But there is no single standard for managing APIs and, thus, teams cannot rely on tools alone to solve security issues. No single product can fix every problem for every language, framework, or context of an API environment.

More on Application Security

Questions and answers

The Rise of SaaS-App Risk and What to Do about It

by Nick Harrahill

IT SECURITY GURU INSIGHT

Katrina Thompson
Data privacy, encryption and IT specialist
Bora

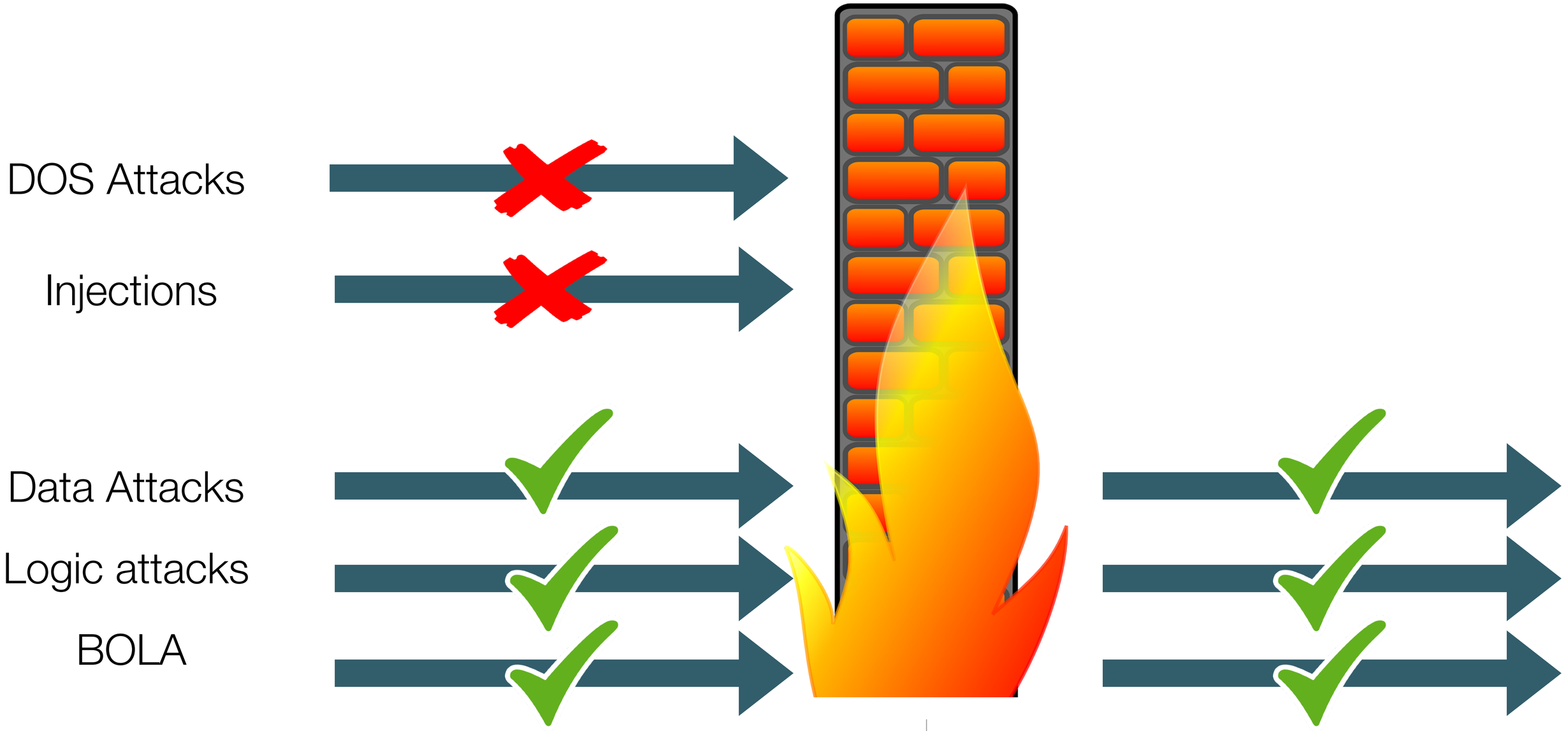
In many ways, considered the "new battleground for cybersecurity" in 2023, APIs can make – or break – a business in the coming year. The fact that they're connectors, that they underpin and pull together the majority of digital services we use daily, makes them prime targets for hacks. The holy grail of a hacker is the ultimate low-risk, high-payout option. Because APIs are the hub for so many useful back-end services, they are a single point of entry and a single point of failure. Getting by in the coming year will be a matter of properly understanding and addressing these inherent threats that, with APIs, just come with the territory.

API Security is a **hot** topic!

Specific API Issues

- Typical vulnerabilities fall into 4 groups:
  - Authorisation/Access Control
  - Authentication
  - Data Control
  - Governance

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



But wait, I have a WAF already !

WAFs are lacking data context
Typically deployed at the edge only

Negative Security Model (Deny List)

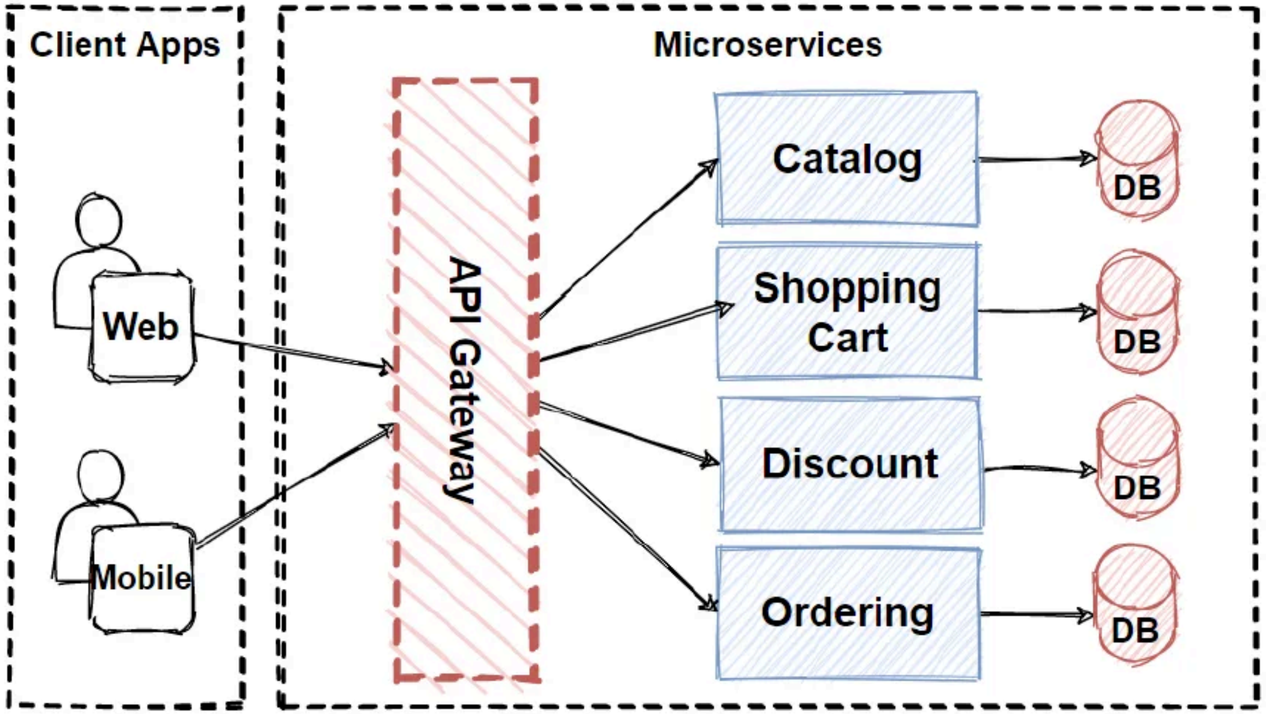
Access Allowed by default

Block access for suspicious traffic

Threats centric

I also have an API Gateway !

- Typical used for authentication management
- Acts as PEP for authorization decisions
- Rate Limiting
- Quota management
- Routing
- Data Transformation/Integration



BY: EREZ YALON ON JANUARY 1, 2020 — 1 COMMENT

As we close out 2019, we at DevOps.com wanted to highlight the five most popular articles of the year. Following is the fifth in our weeklong series of the Best of 2019.

Recent Posts By Erez Yalon

- Breaking Down the OWASP API Security Top 10, Part 2

Show more

Related Posts

- Best of 2019: Breaking Down the OWASP API Security Top 10, Part 1
- WaveMaker Extends Lead in Enterprise Rapid Application

Related Categories

- Blogs
- DevOps Practice
- DevSecOps

As a result of a broadening threat landscape and the ever-increasing usage of APIs, the OWASP API Security Top 10 Project was launched. From the start, the project was designed to help organizations, developers and application security teams become more aware of the risks associated with APIs. This past September, the OWASP API Security

Now people start to realise the problem is real

Fall 2019

APIs are popping up like mushrooms

How do I keep track?

You can’t protect what you don’t know!

✓API Catalog
✓API Governance
✓Current API Security Status

So, there was API Discovery

- Mostly handled via traffic/logs analysis using ML
- Tracks requests over a period of time
- Classifies data
- Useful for behavioral patterns detection
- Zombie APIs detection

BUT HOW DO WE FIX THE ROOT ISSUES ?

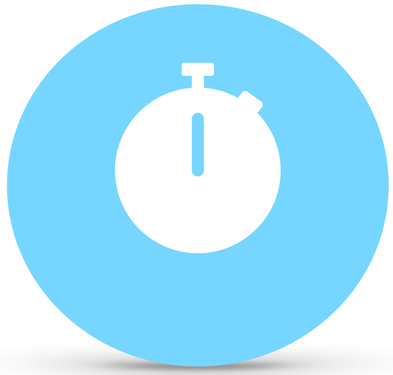
No Magic Solution

You have work to do !

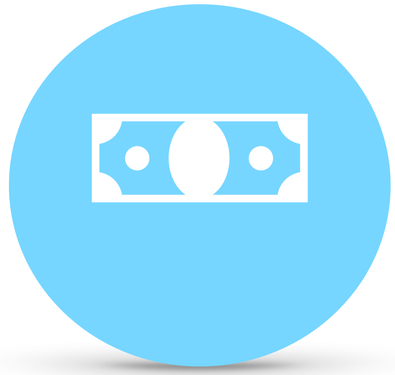
SHIFT LEFT

=

IMPROVED SECURITY

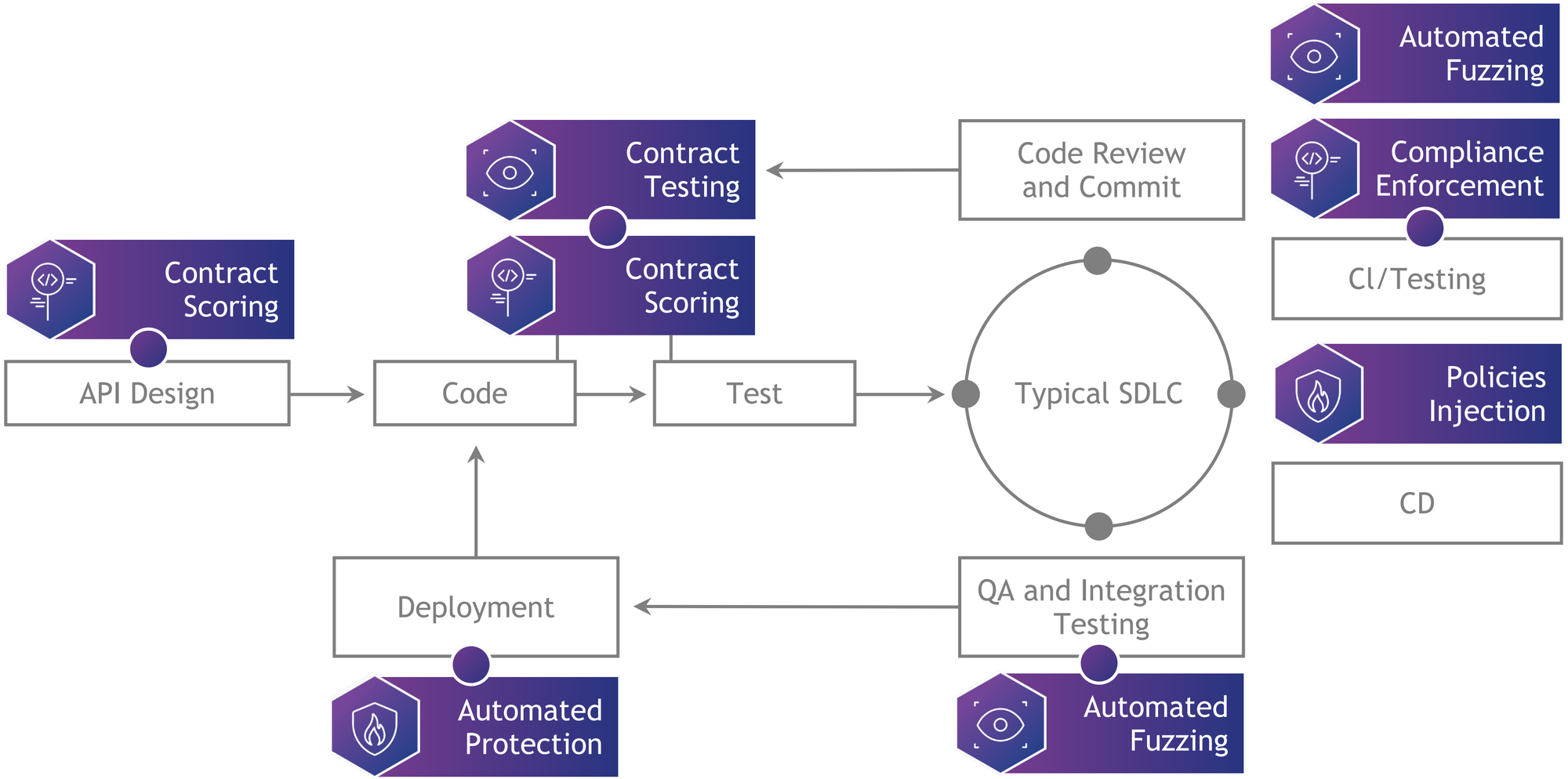


FASTER DELIVERY



REDUCED COST

We need to introduce security every step of the way



Positive Security Model for APIs

- Define expected and reject the rest
- Who can talk to whom
- Authentication and authorization
- Expected data coming in and going out

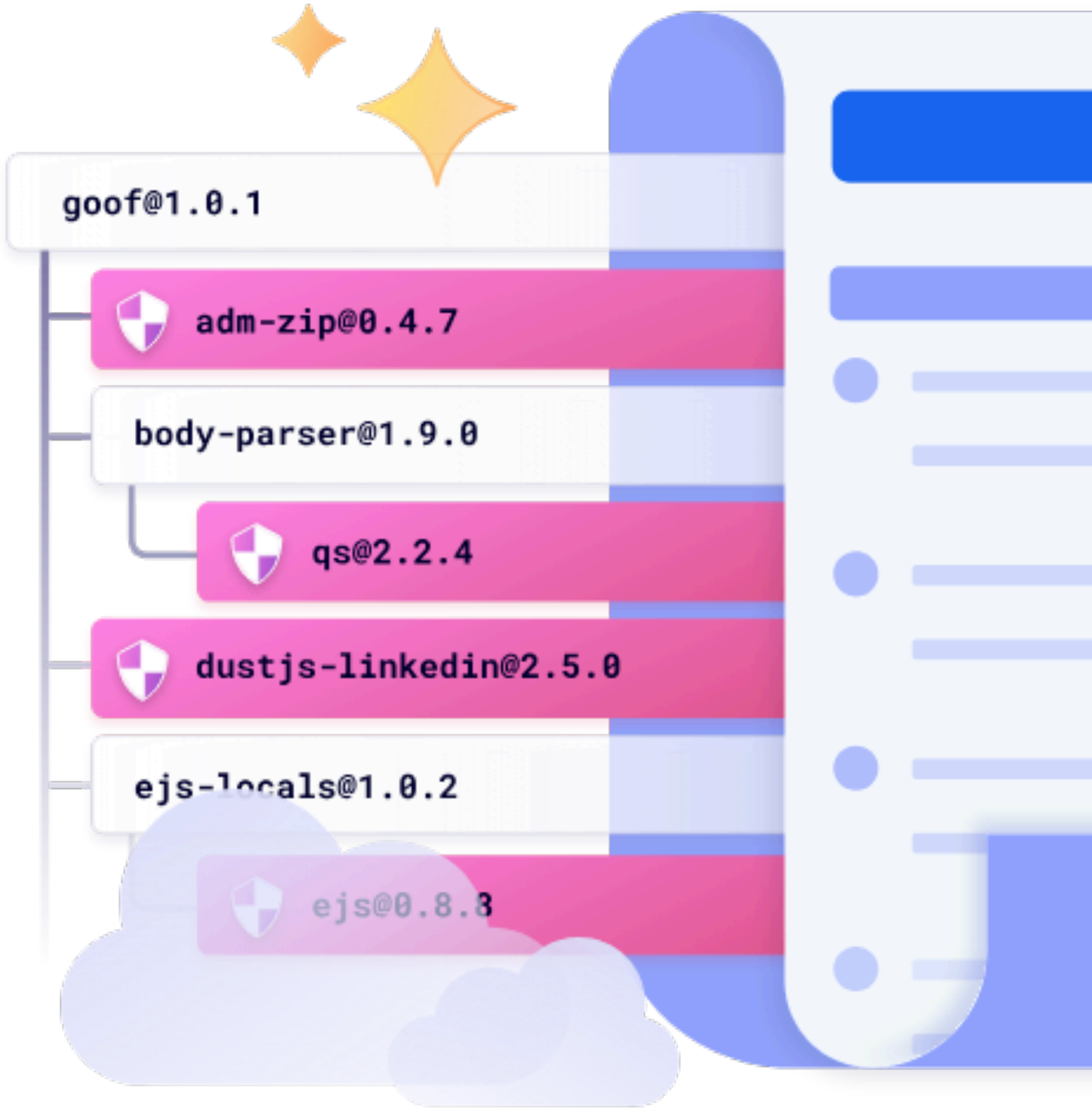
OPEN API INITIATIVE

DEVELOPMENT
working with
APP SEC

It’s not only about tools, it’s about people and processes.

Last thing: control the supply chain

- Docker Images
- Third Party Libraries (especially OSS)
- APIs !!



Application Security is **hard**!

For everyone. Invest in **educating everyone.**

CALL TO ACTION!

Use OWASP API Top 10 as framework for design and testing

Start with your critical APIs

Start worrying about API Security at design time

- ✓ A vulnerability discovered at production time costs up to 30x more to solve

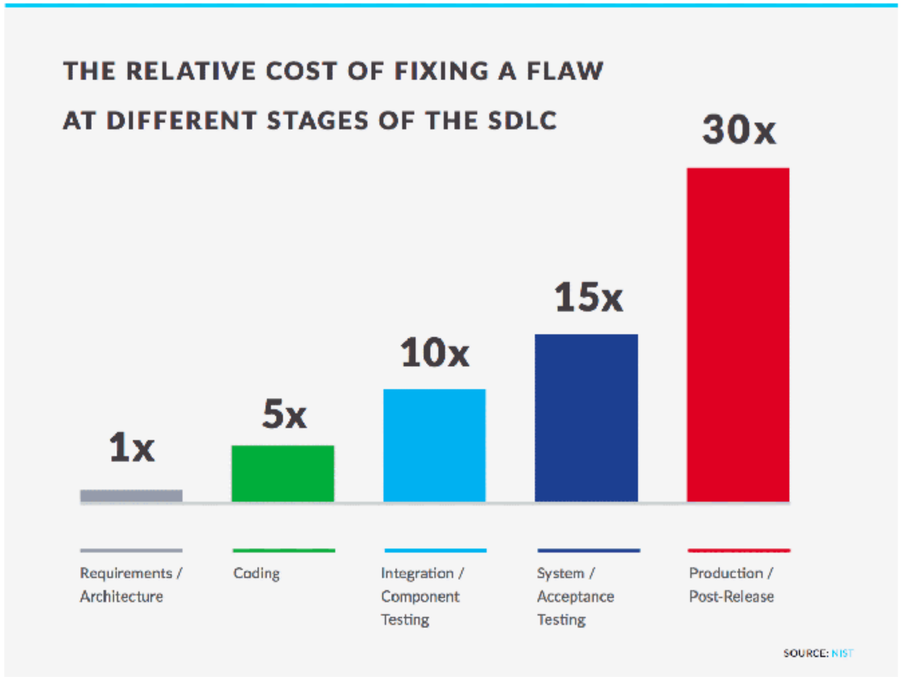
Hack yourselves leveraging API contracts

- ✓ For each functional test, create 10 negative tests
- ✓ Hammer your APIs with bad data, bad tokens, bad users

Automate Security

- ✓ Inject Security into DevOps practices and don't rely on manual testing of APIs.
- ✓ Only solution to scale and have avoid human errors

https://www.helpnetsecurity.com/2020/05/20/devops-software-development-teams/



"I think security, in most cases, is not a single person's specialization. Security must be a practice of every member of the team from the frontend developer to the system administrator (also non tech roles)."

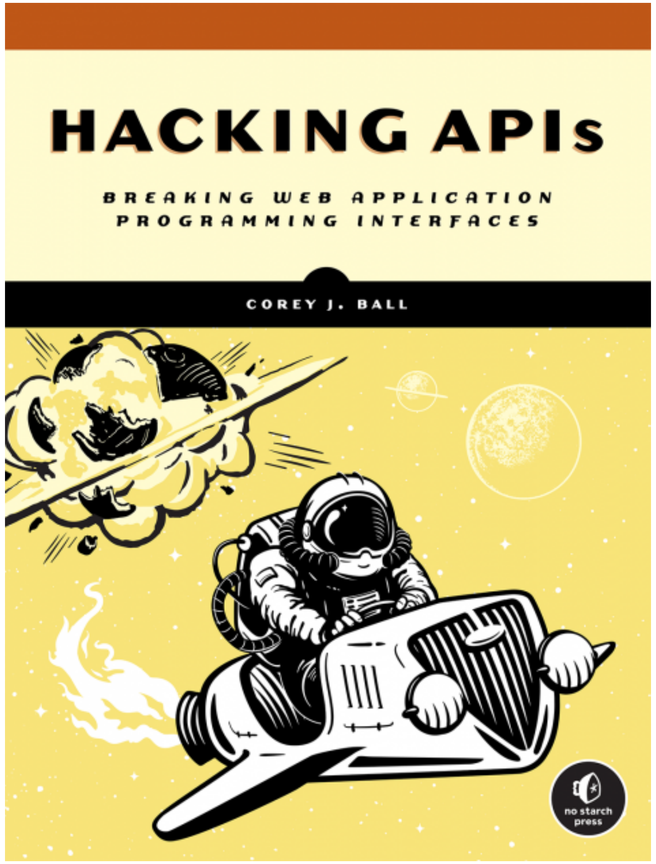
From: Gitlab DevSecOps report - 2021

Learning more

APISecurity.io

https://apisecurity.io/

“Hacking APIs” - Corey Ball



https://nostarch.com/hacking-apis

Learning Application Security

Buy the book