APIs – Security & Performance – How to Avoid Getting in the News

Presented by
Adam Sandman
Software Test Professionals (STPcon)
April 1-4, 2019 | San Francisco, CA

inflectra®

1

About Me

- Adam Sandman was a programmer from the age of 10 and has been working in the IT industry for the past 20 years.
- Currently Adam is a Director of Technology at Inflectra Corporation, where he is interested in technology, business and innovation.
- Adam lives in Washington, DC, USA

inflectra®

2

Agenda

- Overview of APIs
- Why Test for Security & Performance
- Planning for Success
- Performance
- Security
- Questions

inflectra®

3

Takeaways

1. Learn about how you should plan to test the security of your API endpoints
2. Learn techniques and methods for testing and measuring the performance of your APIs
3. Gain a comprehensive understanding of the factors that can lead to poor performance and security of your APIs
4. Have practical tools and techniques that you can use to test your APIs for security and performance, and ideas that you can share with your developers.

inflectra®

4

The API Economy

Why APIs Are Vital for Today's Businesses?

inflectra®

5

First, What is an API?

inflectra®

6

API = Application Programming Interface

inflectra®

7

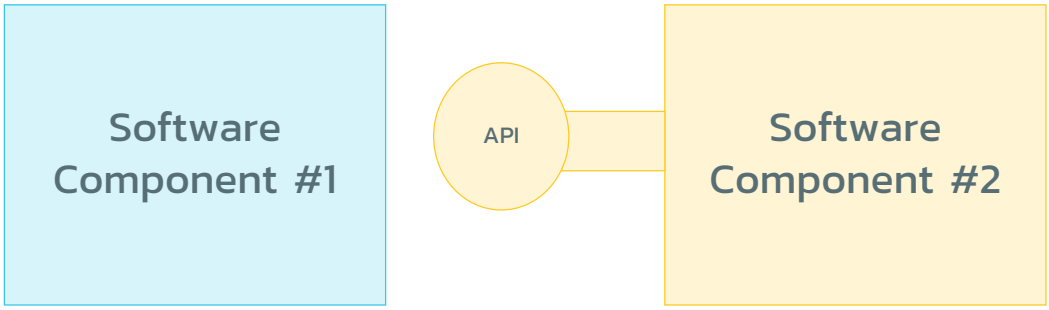
OR

A way for one piece of software to use the functionality of another piece of software

inflectra®

8

How Does that Work?



inflectra®

9

What is So Special?

- The API provides what's called an "interface"
- It acts like a contract between the software using the API, and the software providing the API
- Different people can develop their own implementations of the same API.
- Developers of Component #1 don't have to understand the inner workings of Component #2, just the implementation

inflectra®

10

Why Test for Security or Performance?

Warning: Not for the Faint Hearted!

inflectra®

11

Performance:

inflectra®

12

Example #1

HealthCare.gov

- October 2013 - healthcare.gov website launched
- Most website users experienced crashes, delays, errors, and slow performance
- First Day
  - 4,000,000 unique visitors
  - Only 6 successful signups
  - 0.00015% conversion rate (!)
- American taxpayer spent ~ $840 million to build site
- Problems traced back to back-end data services hub & APIs

inflectra®

13

Example #2

J.CREW

- J.Crew's website crashed during 2018 Black Friday sales shopping.
- Customers were complaining on Twitter that they were unable to add items to their carts online.
- It could have cost the company over $700,000 in lost sales in one day, plus immeasurable damage to the brand
- Traced back to insufficient capacity in payment gateway and shopping cart APIs

inflectra®

14

Security:

15

Example #1

- IRS Transcript API Breach in 2015
- 350,000 taxpayer accounts were illegally accessed using the "Get Transcript" API
- Almost 610,000 taxpayers "were at heightened risk of future identity theft"
- Once authenticated, you could call the API to get access to the taxpayers' information without authorization checks

16

Example #2

miSafes

- miSafes Kids Watches allowed attackers to see API traffic
- Could geo-locate the children using GPS
- Could make a phone call to the child
- Could listen in on the child
- Retrieve personal data on child (name, DOB, age, etc.)
- No TLS security implemented on API
- No post-authentication authorization checking
  - Can enumerate all of the IDs

inflectra®

17

Impact

inflectra®

18

No One Wants to Wake Up To….

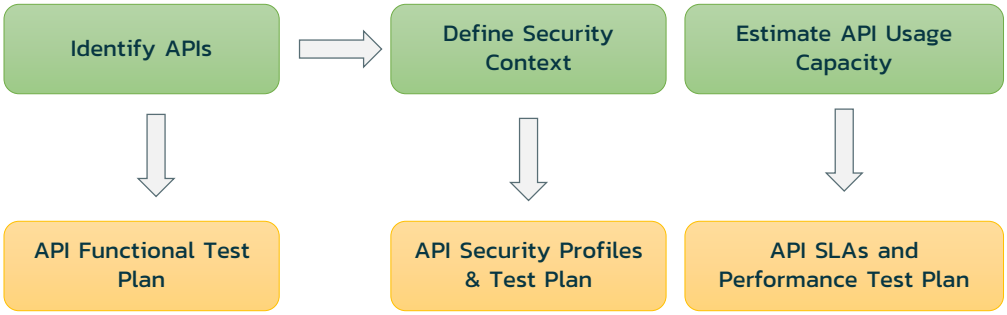
inflectra®

Planning for Success

First You Need to Plan for Testing your APIs

inflectra®

The API Testing Plan



inflectra®

21

Scope the Effort

- Identify the API Endpoints
  - How Many Versions (v1, v2, v3)
  - How Many Types (SOAP, REST)
  - How Many Formats (XML, JSON)
- Identify the security context of each API endpoint
  - Highlight those with access to especially sensitive data
- Estimate the usage capacity for each of the APIs
  - Identify those that are business critical
  - (e.g. store locator vs. payment API)

inflectra®

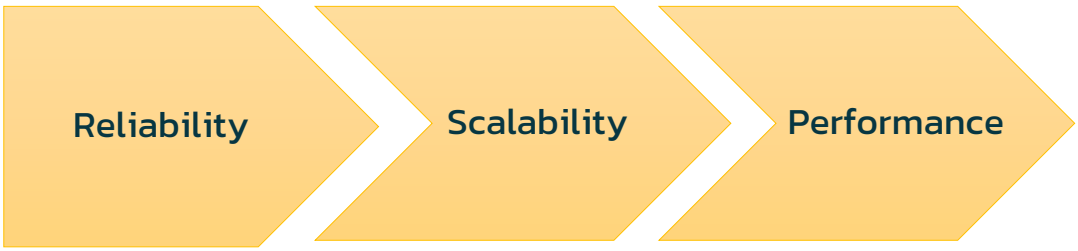
22

API Performance Planning

inflectra®

23

Performance Engineering Plan

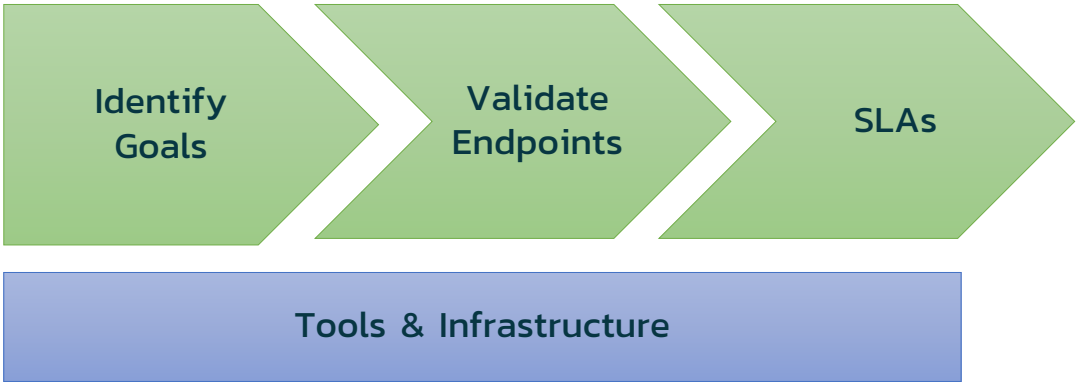


How does an API provider make sure it is fit for purpose and can deliver on defined Service Level Agreements (SLAs)

inflectra®

24

Performance Engineering Plan



inflectra®

25

1. Identify Goals

- Establishing Baseline Metrics
- Understand How Changes Affect System
- Validate Performance
- Validate Scalability
- Stress Test to Determine Reliability
- Identify Bottlenecks
- Plan for Growth

These are NOT the same goals. You need to choose!

inflectra®

26

2. Identify & Validate Endpoints

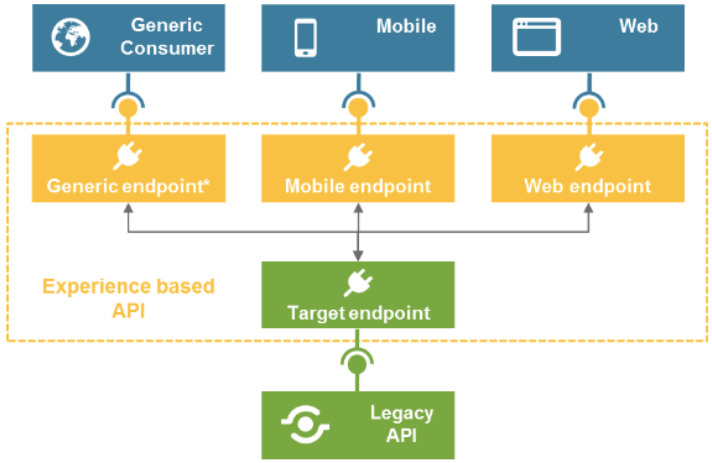


Image reproduced from: https://dzone.com/articles/api-integration-patterns-experience-based-apis

inflectra®

27

3. Confirm SLAs

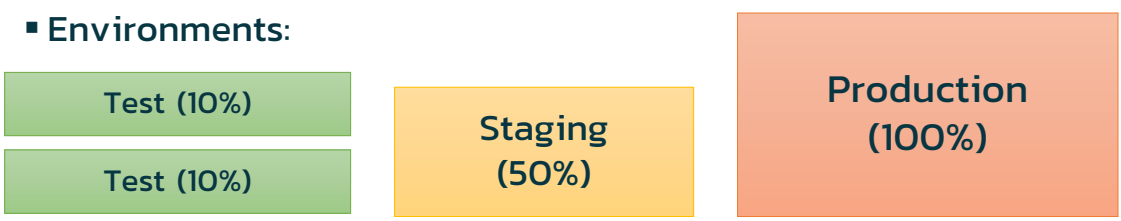
- Document any external contractual SLAs
  - E.g. API must support 1 million requests per second (RPS)
- Monitor existing traffic patterns
  - Distribution by day/time
  - Distribution by API endpoint
  - Distribution by geography
  - Distribution by user
  - Etc.
- Craft internal SLAs

inflectra®

28

4. Tools & Infrastructure

- Understand the tools you will need
  - Load testing
  - Performance monitoring
  - Environment management
- Environments:



inflectra®

29

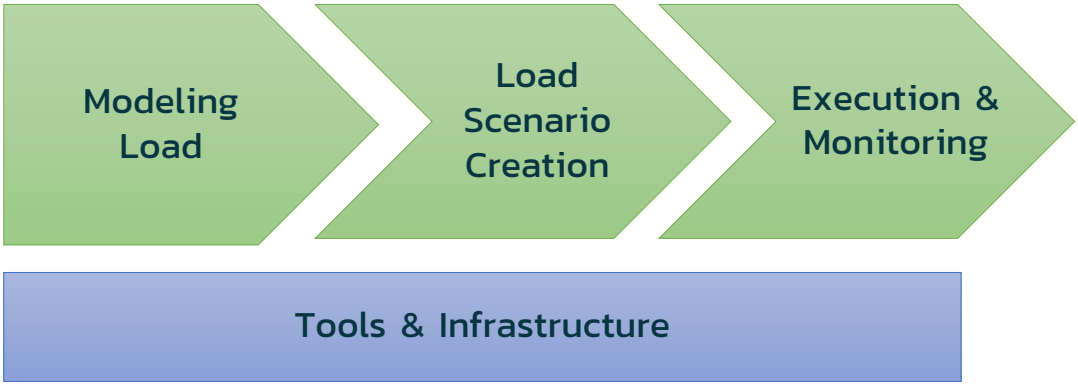
API Performance Testing

Configuration & Execution

inflectra®

30

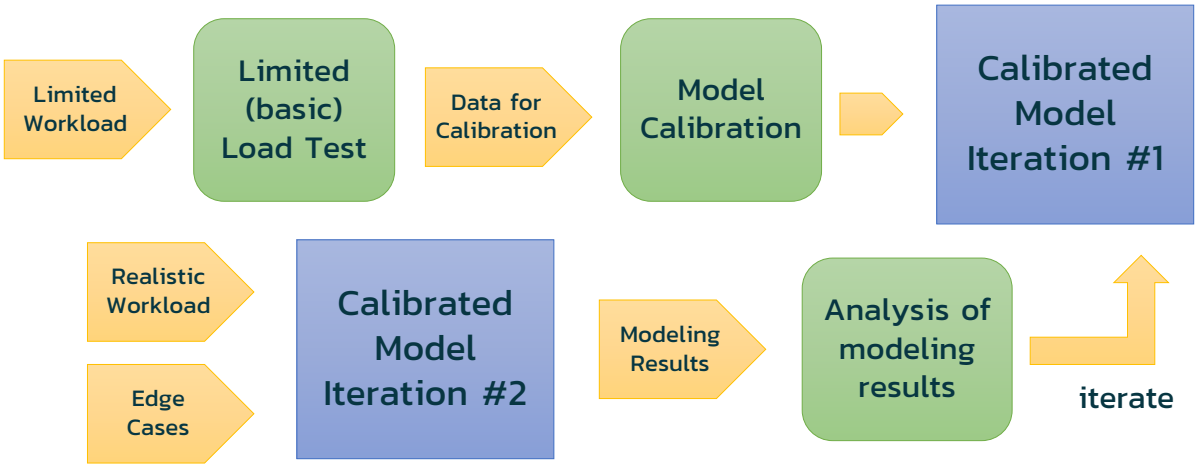
Performance Configuration & Execution



inflectra®

31

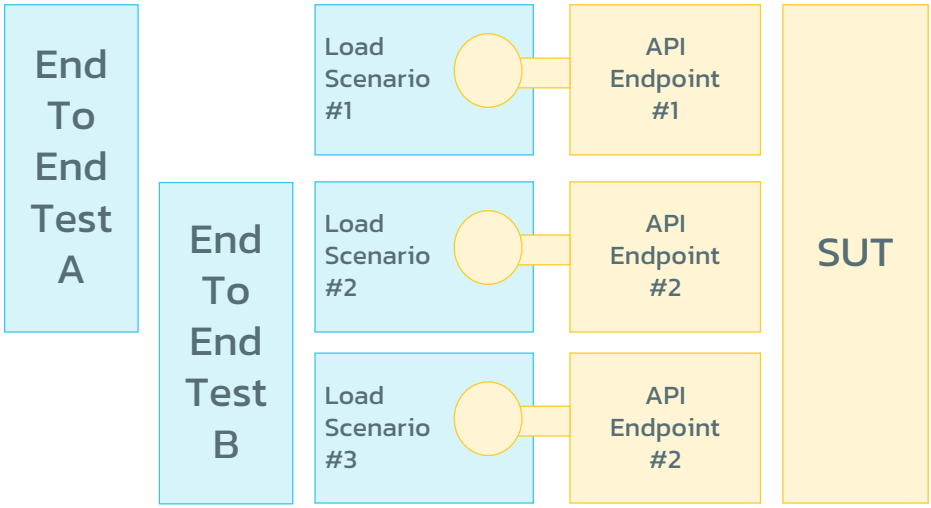
Modeling Load & Throughput



inflectra®

32

Load Scenario Creation



inflectra®

33

Execution & Monitoring

1. Exploratory API load testing
   - Individual scenarios
   - Combine into ad-hoc end to end tests
2. Automated API load testing
   - Deploy into CI/CD pipelines
   - Integrate with test management platforms
   - Standardize the end to end tests

inflectra®

34

Tools & Infrastructure

- Success of load testing depends on proper choice of tooling, and sufficient infrastructure for your needs and goals:

Commercial

NeoLoad

dynatrace

Open Source

Gatling

APACHE JMeter™

k6

inflectra®

35

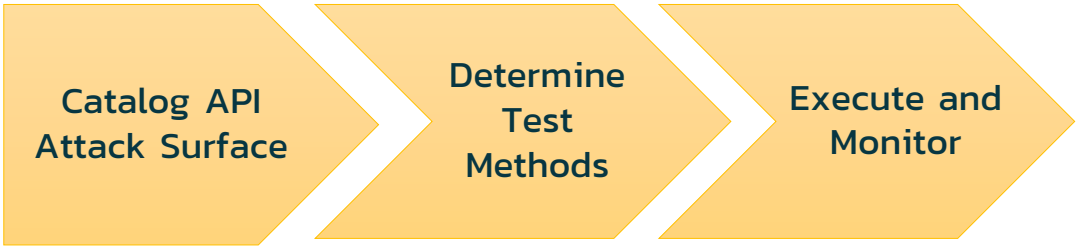
API Security Testing

Techniques and Methods

inflectra®

36

API Security Testing Plan



How does an API provider make sure it is fit for purpose and can deliver on defined Service Level Agreements (SLAs)

inflectra®

37

Differences with Performance

- Load testing is more business driven
  - You can have 30% less performance and accept the business risk
- Security testing is more binary
  - You are secure or you are hacked
  - You have less "choice" over how many types of tests and approaches to deploy

inflectra®

38

Catalog API Attack Surface

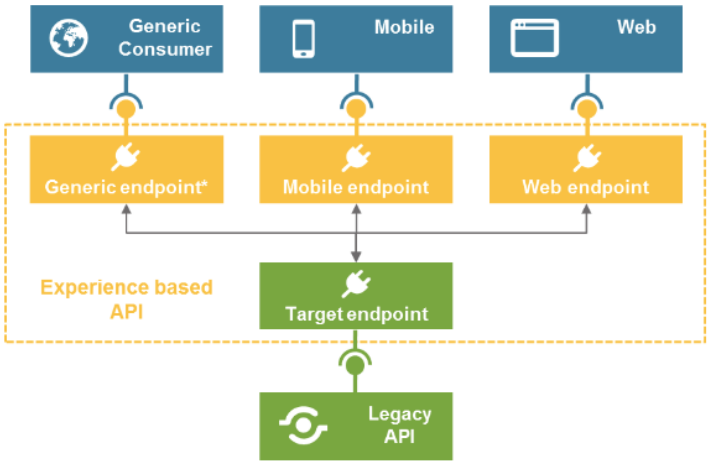


Image reproduced from: https://dzone.com/articles/api-integration-patterns-experience-based-apis

inflectra®

39

Determine Test Methods

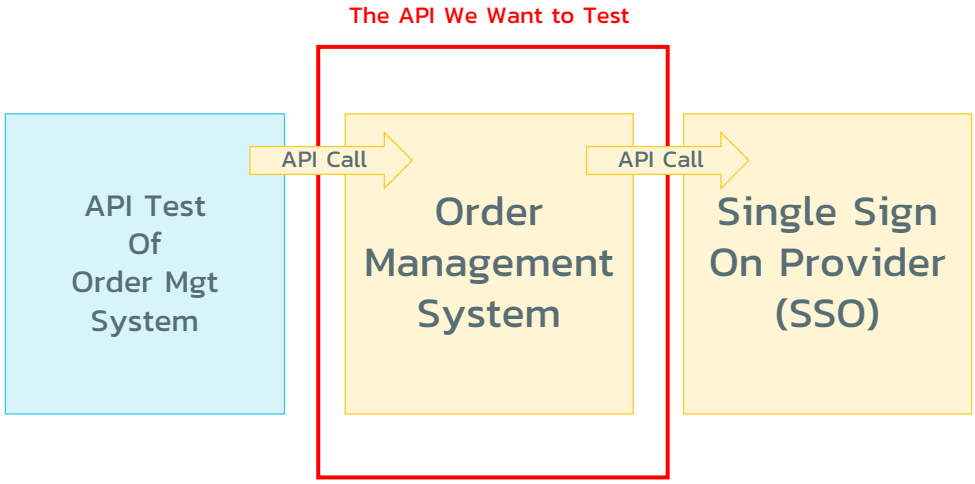
- Authentication
- Authorization
- Null Pointers
- Buffer Overruns
- Data Discovery & Enumeration
- Fuzz Testing
- Command Injection
- Parameter Tampering

Determine which ones make sense for your APIs

inflectra®

40

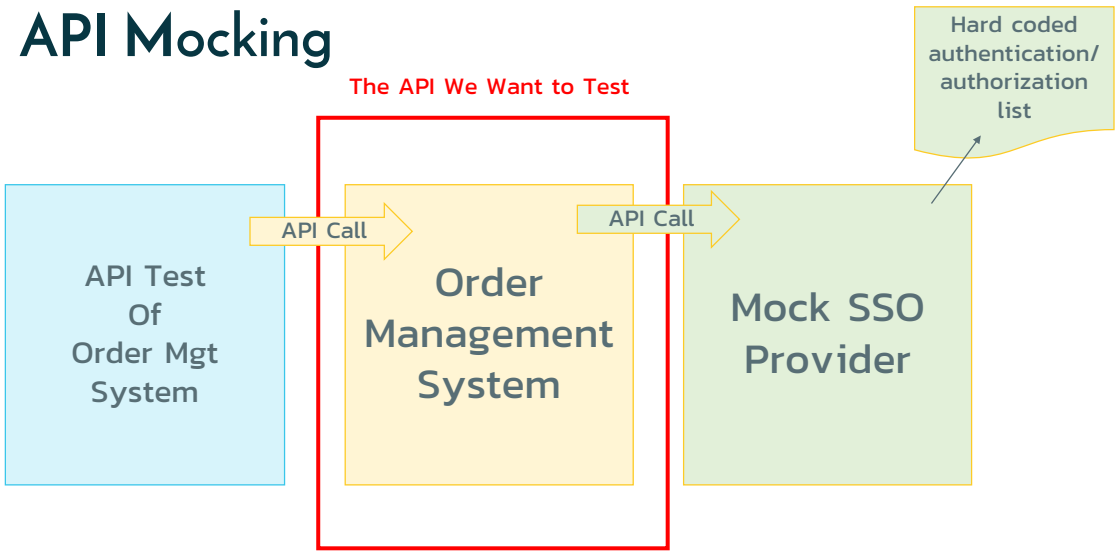
Use of API Mocking



inflectra®

41

API Mocking



inflectra®

42

Execute and Monitor

- Perform deep tests and scans of your APIs
- Incorporate into CI/CD pipeline if feasible

- Once deployed into staging/prod environments:
  - Combine with penetration testing
  - Combine with vulnerability testing
    - (e.g. use of TLS 1.0)
    - (e.g. use of unpatched Tomcat)

- Integrate with test management

inflectra®

43

Tools & Infrastructure

- You can use general API testing tools, or choose ones that are specifically designed for security testing:

Specialized

BURPSUITE

Vooki

OWASP ZAP

or

General

SoapUI

POSTMAN

Rapise®

inflectra®

44

Wrap Up & Final Thoughts

- APIs are a building block of the modern economy
- When they fail it results in real-word consequences
- You need to build security and performance into your test plans right from day one
- A well thought out plan, with appropriate tools and infrastructure, mapped to your business goals and SLAs will keep you out of the papers....

inflectra®

45

Questions?

inflectra®

46

Thank you for attending this workshop/session.

Please fill out an evaluation form.

inflectra®

47