Pentesting on steroids using performance monitoring

BSides Lisbon, 2022

Jean-Baptiste Aviat, Datadog

Staff Engineer for Security Products

sqreen CTO & Co-founder

Former (Red Team), pentester

Email: jb@datadoghq.com

Twitter: @jbaviat

What is ~~performance monitoring~~?

What is observability?

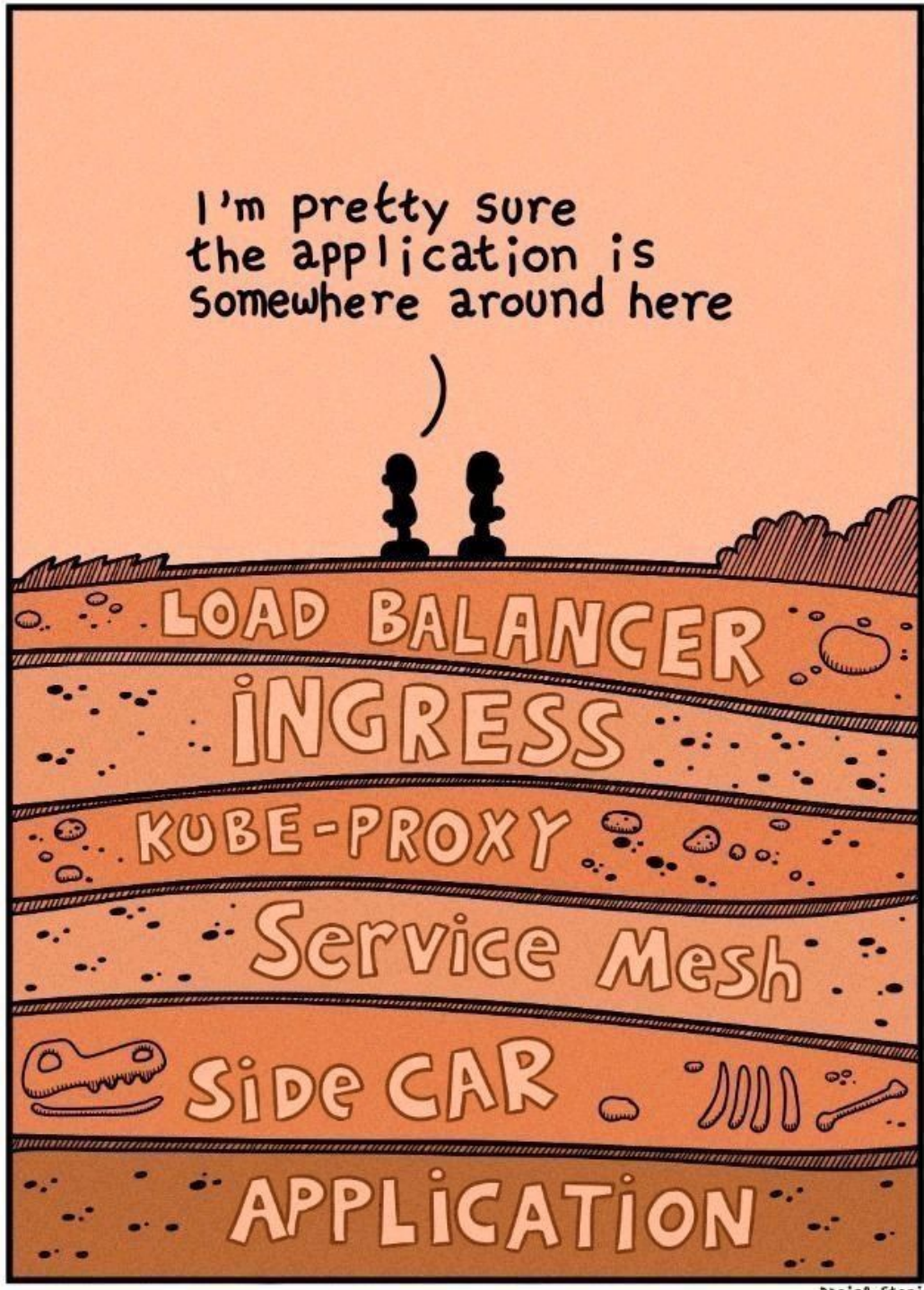
And why do engineering teams care about it?

Building and maintaining complex systems

Systems engineers are dealing with grew in complexity

They need specific tools to help them…

- visualize
- understand the flows
- debug
- monitor deviations



DATADOG

Attacking complex systems

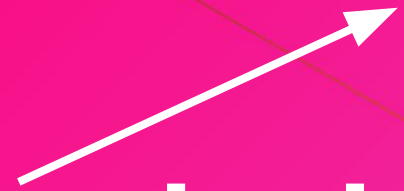
Lots the needs are similar with engineering needs:

- Accelerate recon
- Facts instead of hypotheses
- Observe systems internal response to stimuli
- Discover hidden components

DATADOG

How do we do this?

product engineers



How do ~~we~~ do this?

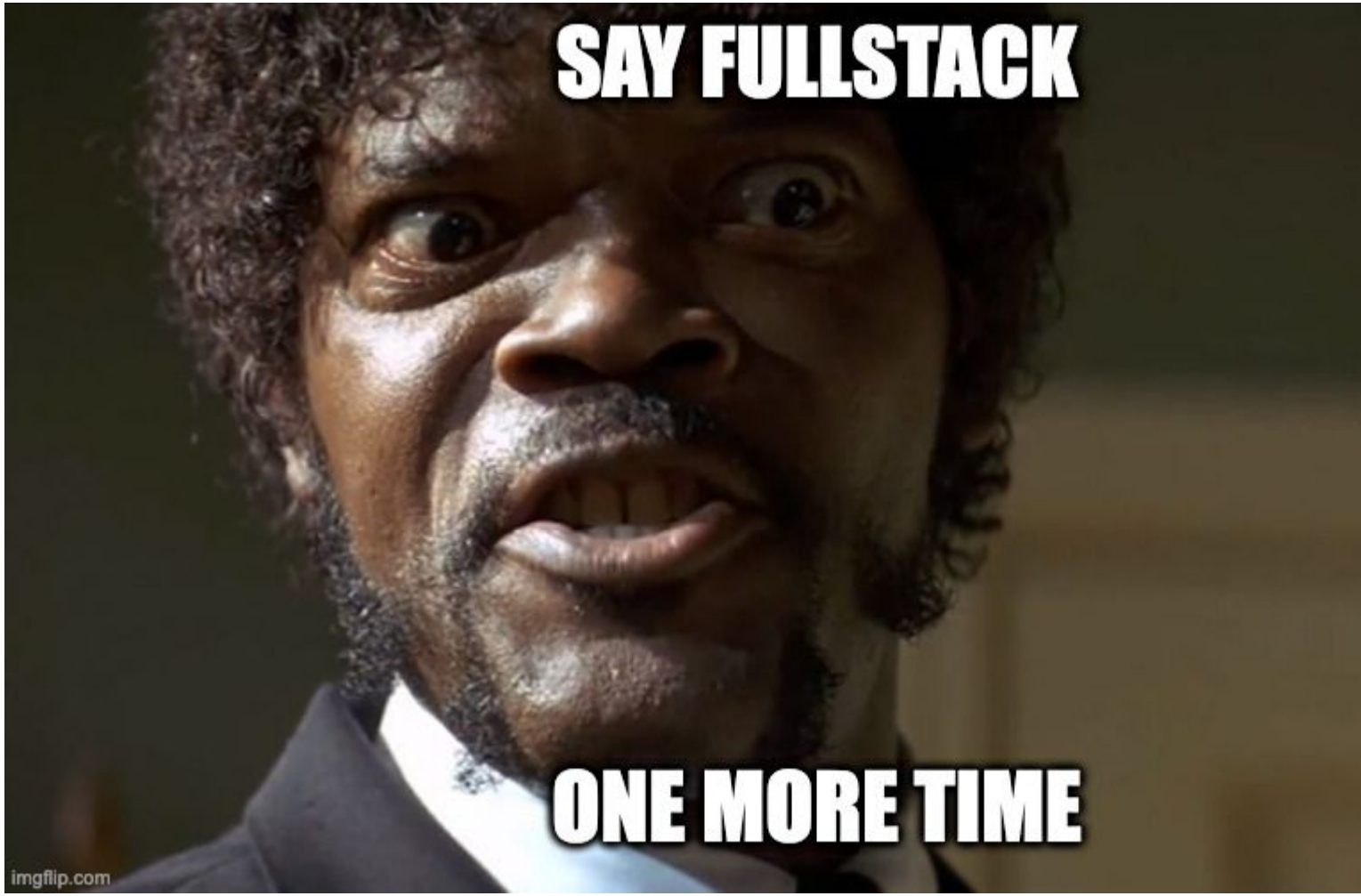
Modern observability products give *full stack* visibility

Data plane

Container orchestrator
Hosts & containers
Applications
Datastores

Cloud control plane

IAM users & permissions
Security settings
Network configuration



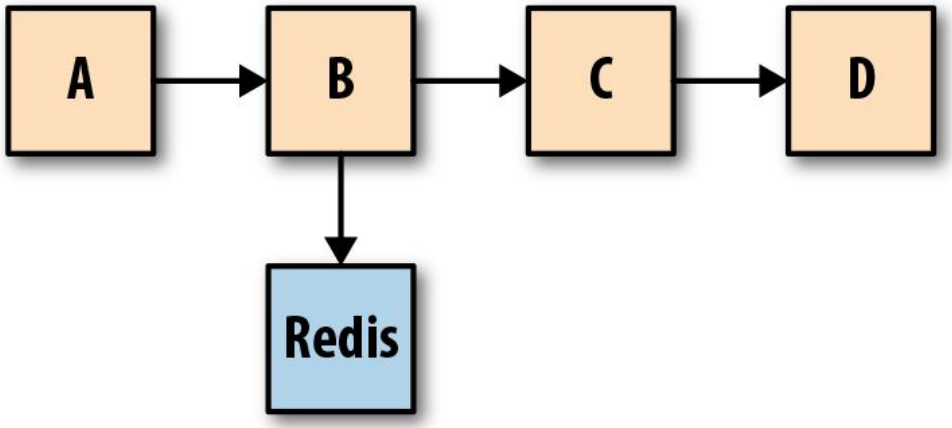
Many paths to observability

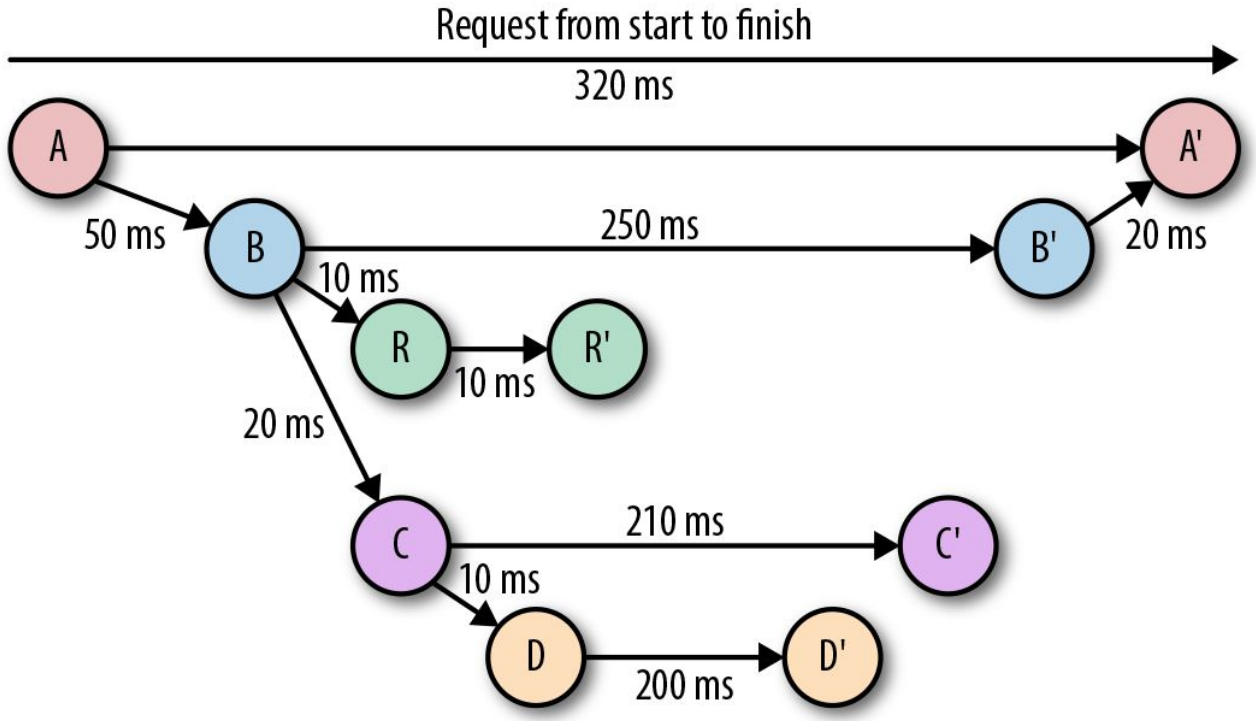
Many products: open source or commercial

Disclaimer: I talk about Datadog - but assume similar capabilities from most other products

Demo of an observability product

How does distributed tracing work?





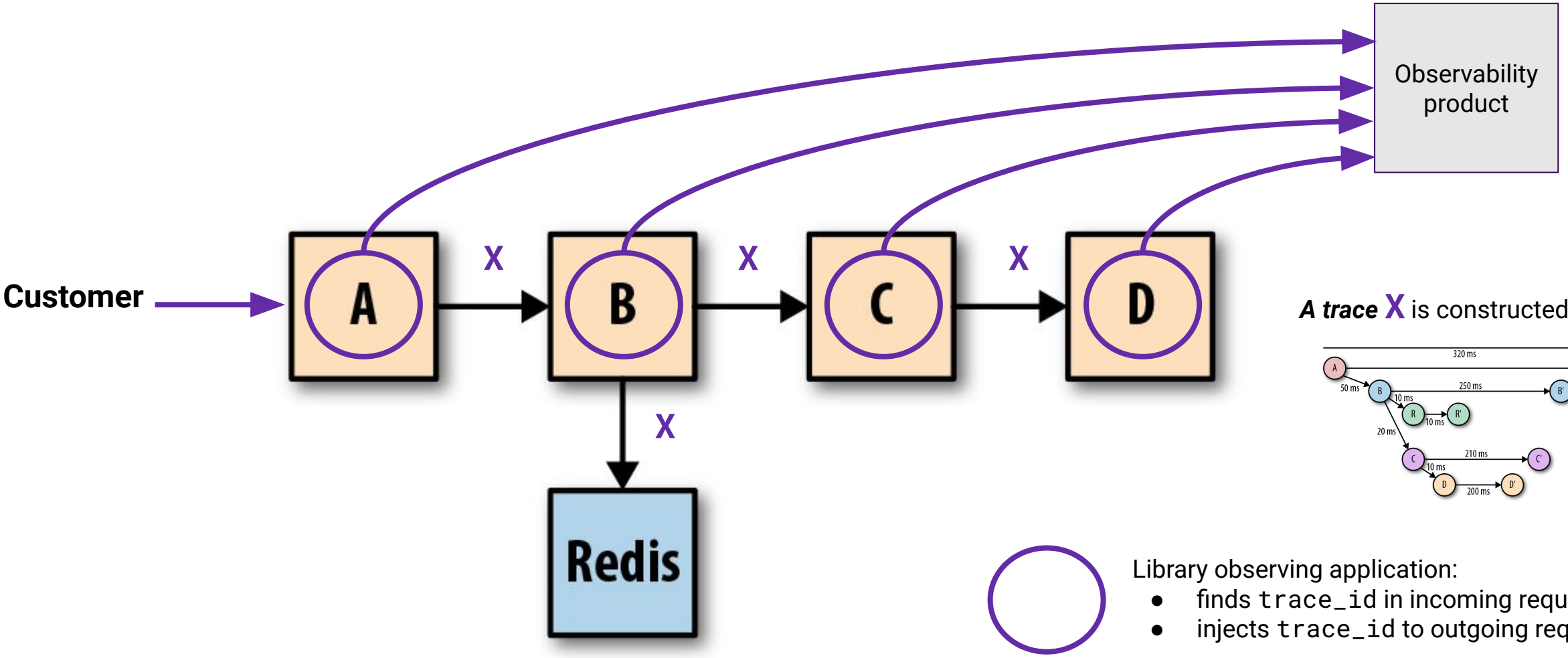
DATADOG

Source: Distributed Systems Observability by Cindy Sridharan, Oreilly

How do APM work?

In-app libraries injecting and propagating an ID

Data centralization



A trace **X** is constructed:

Library observing application:

- finds `trace_id` in incoming requests
- injects `trace_id` to outgoing requests

X trace_id: random number identifying a ***trace***

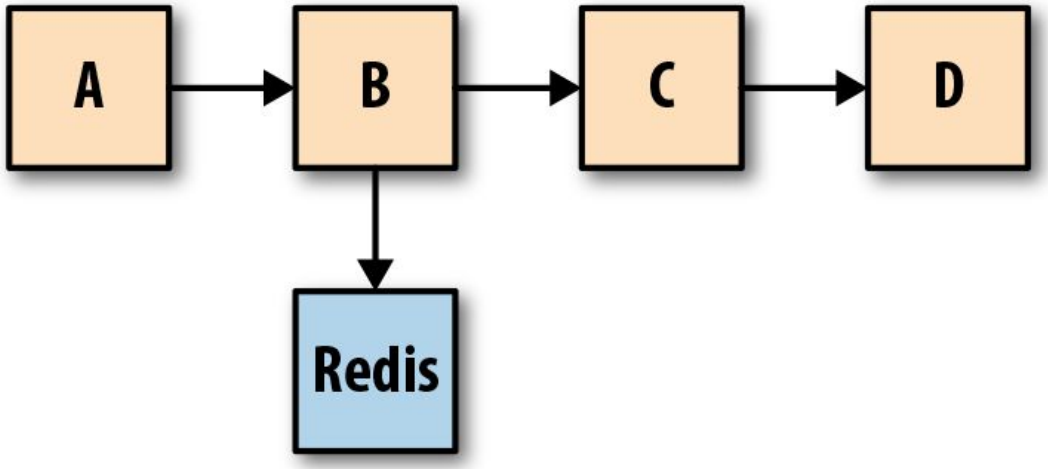
DATADOG

APM is magic!!

APM limitations

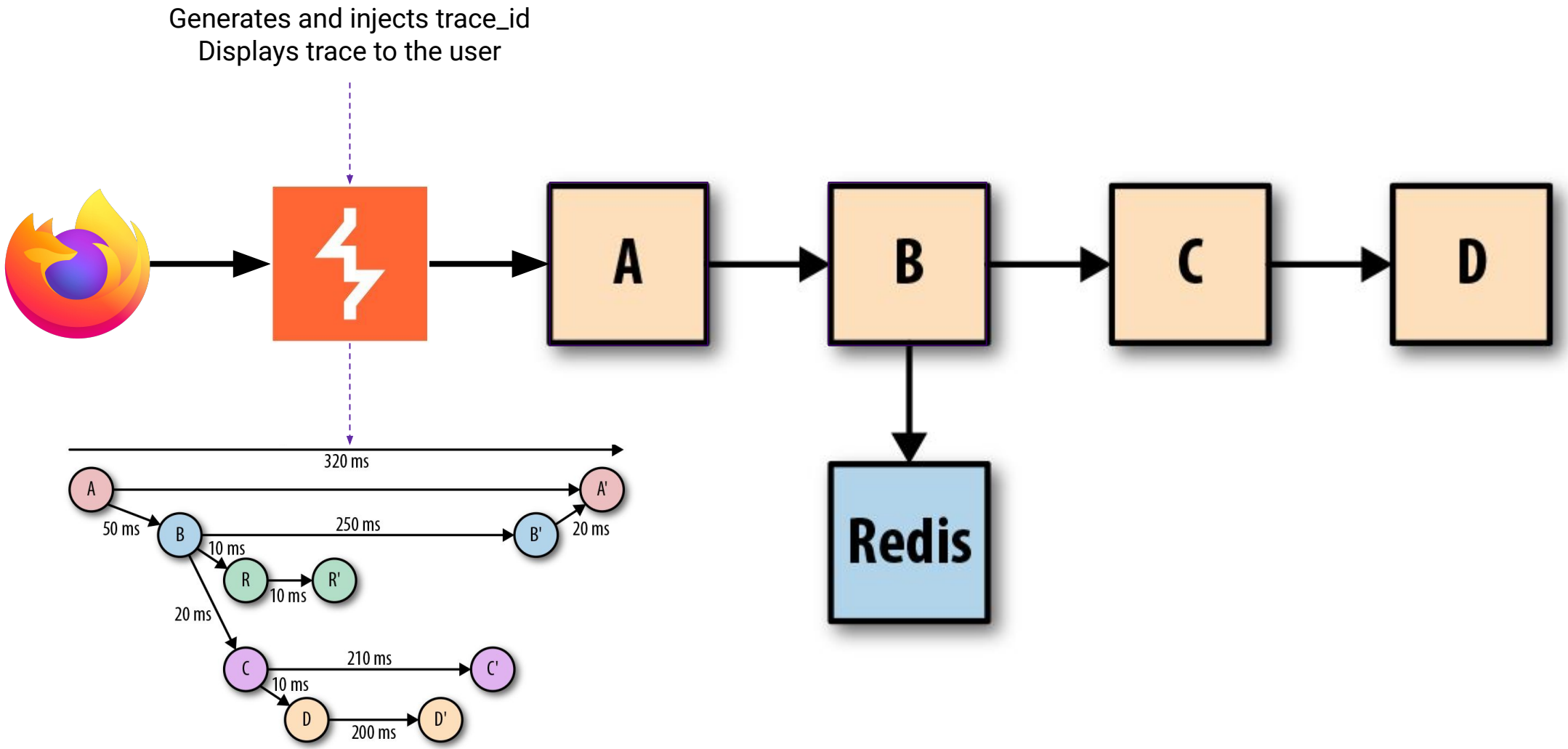
Need to support lots of libraries: if B → C is gRPC, gRPC support is mandatory not to loose C and D

Sampling: ingesting and indexing traces is costly, hence sampling is applied



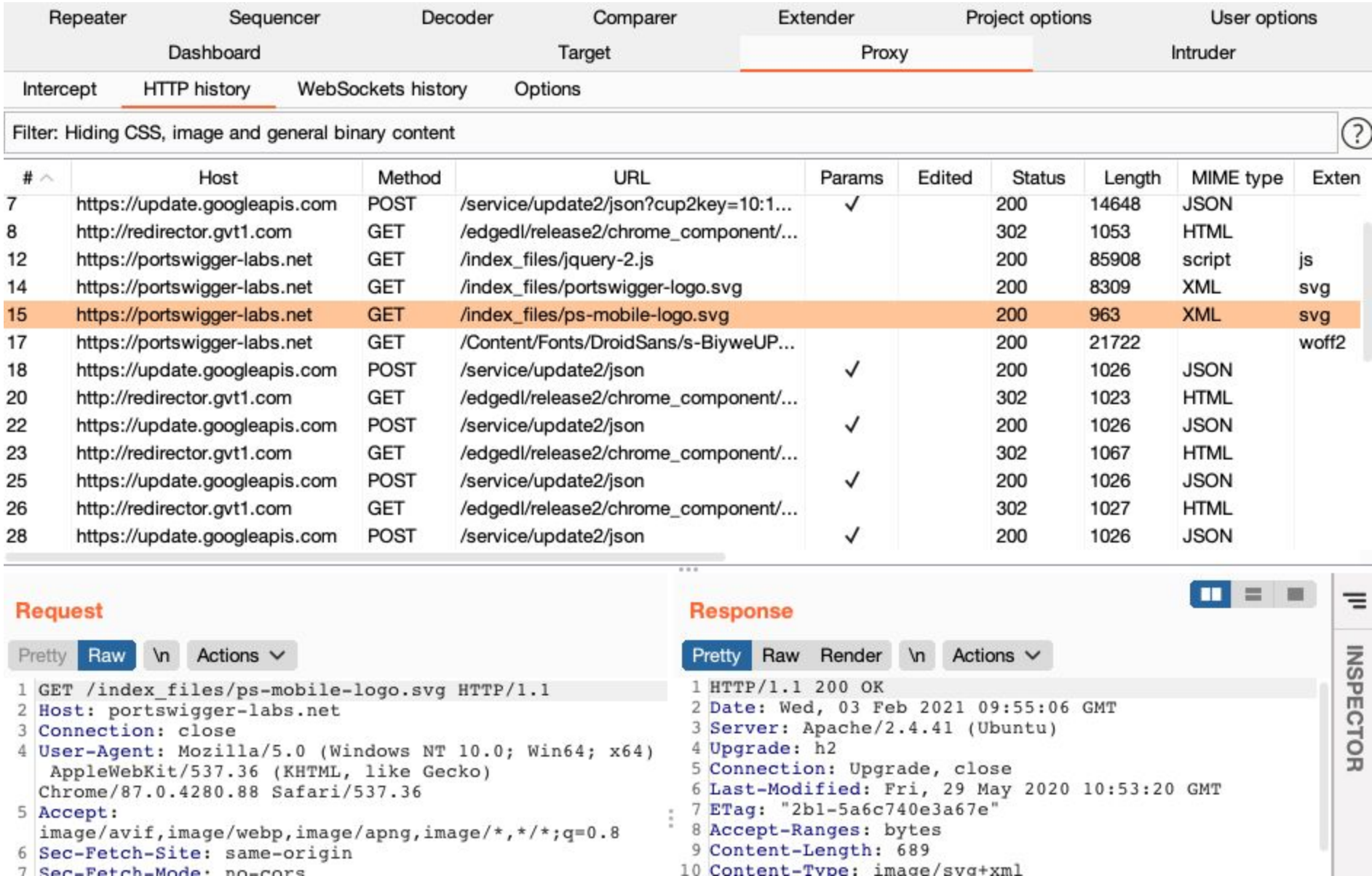
Pentesting with observability

Turn Burp Suite into an APM library



DATADOG

What is Burp Suite?



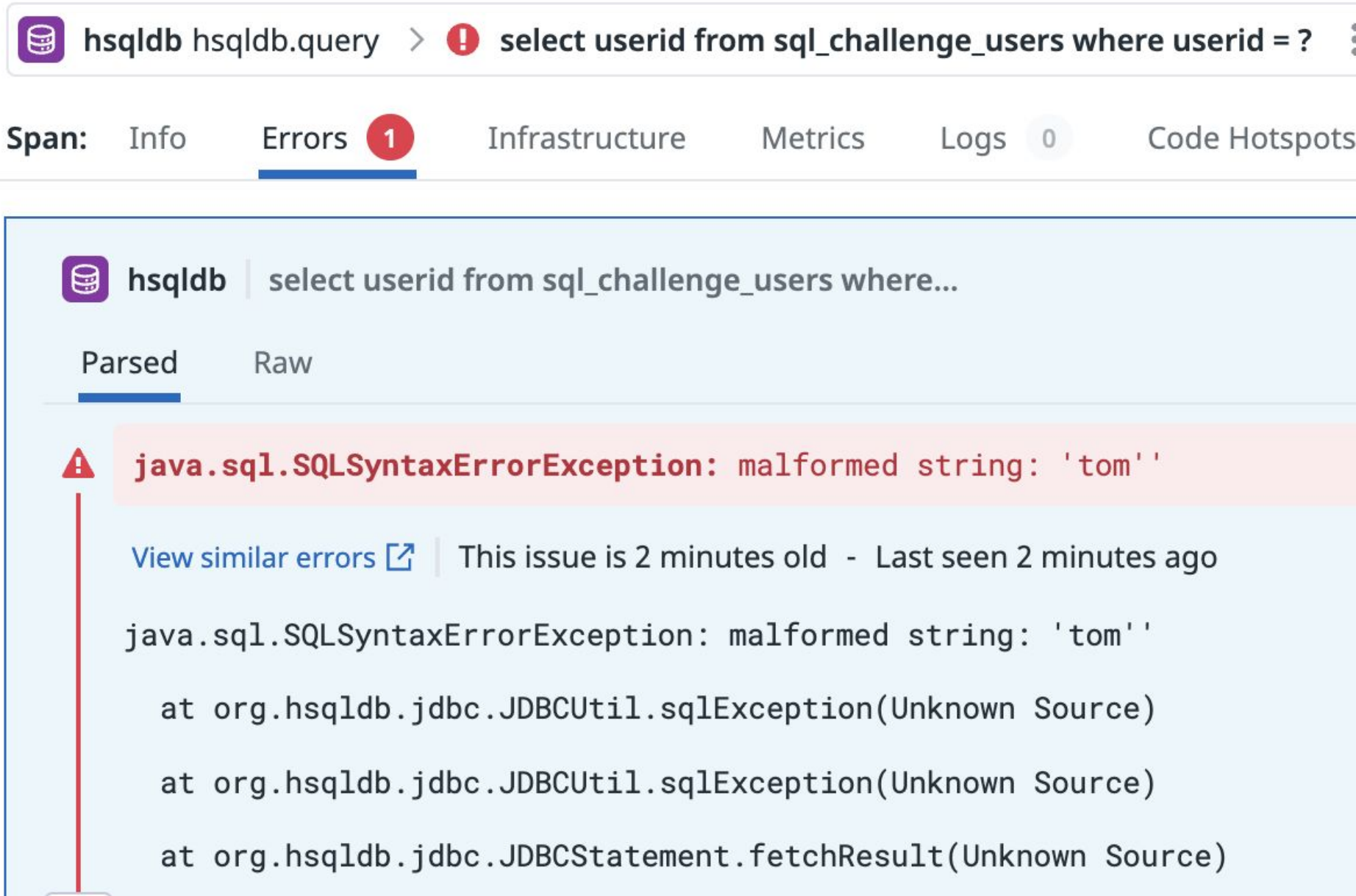
DATADOG

Pentesting x Observability: SQL injection

Demo

Full visibility into SQL and triggered errors

Accelerate SQL injection exploitation by accessing the full query and generated exceptions.



DATADOG

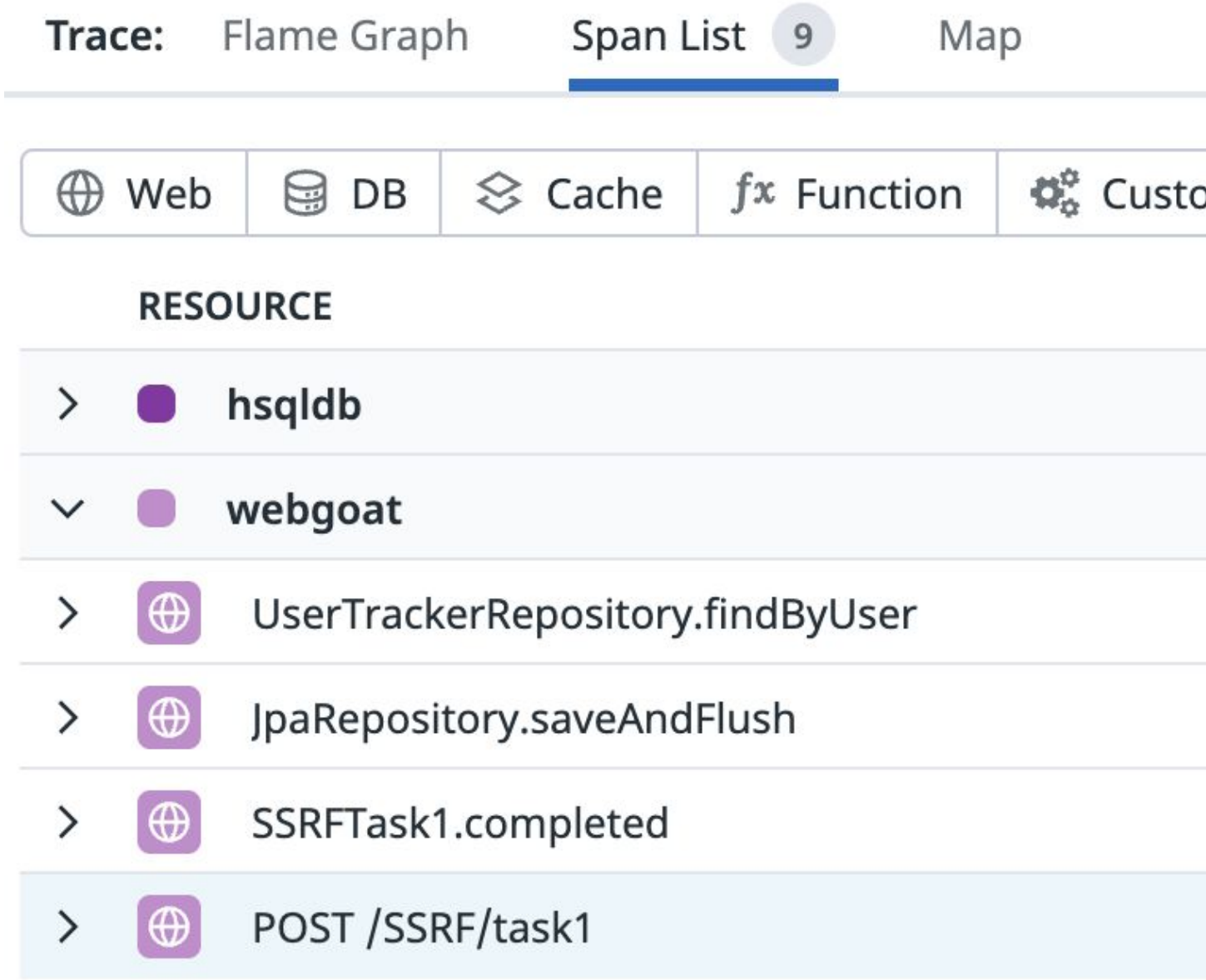
Pentesting x Observability: SSRF

Demo

Pentesting x Observability: SSRF

Understand the actions performed by a endpoint.

Here, no network access limit the exploitability of this SSRF.



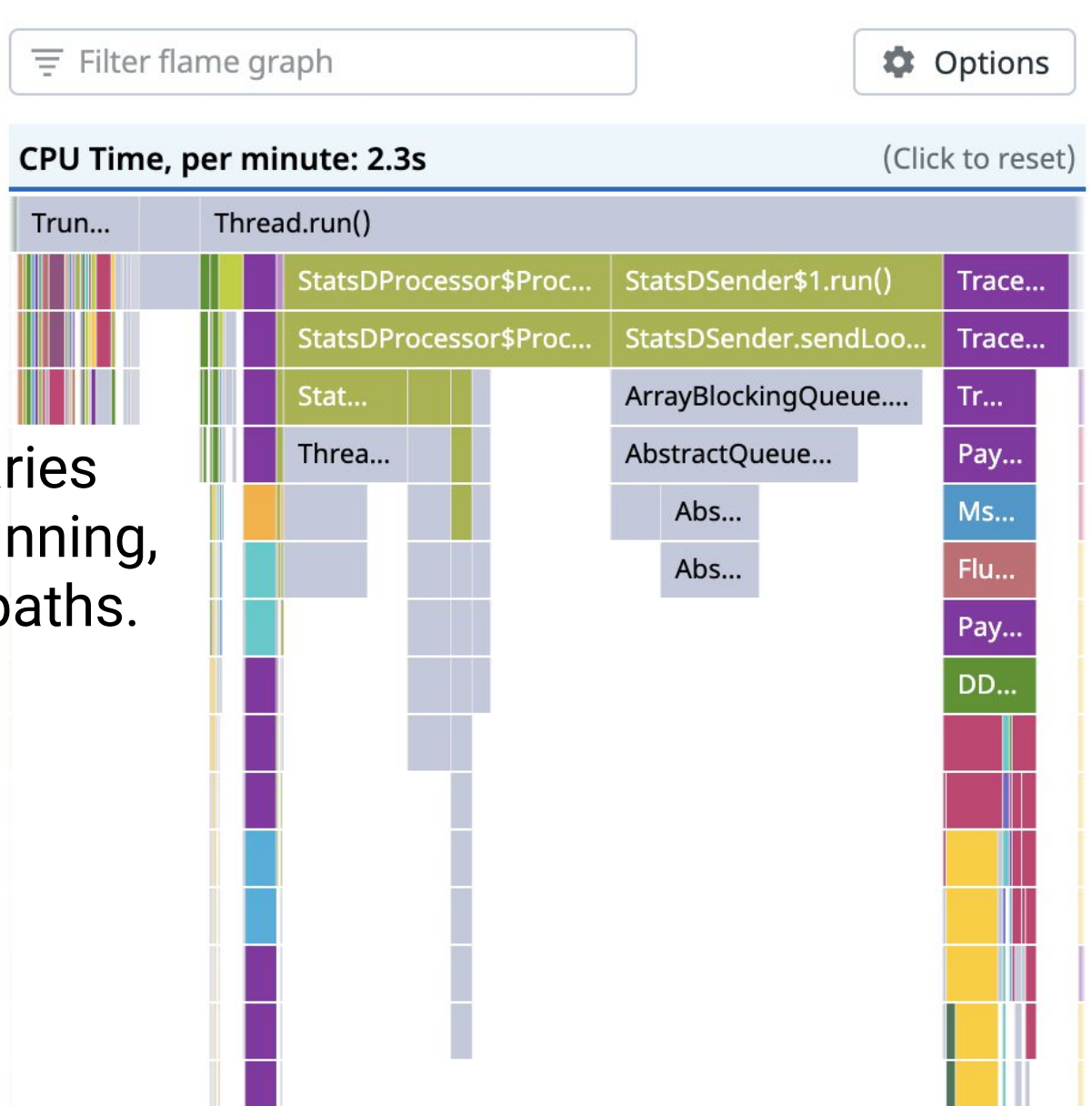
DATADOG

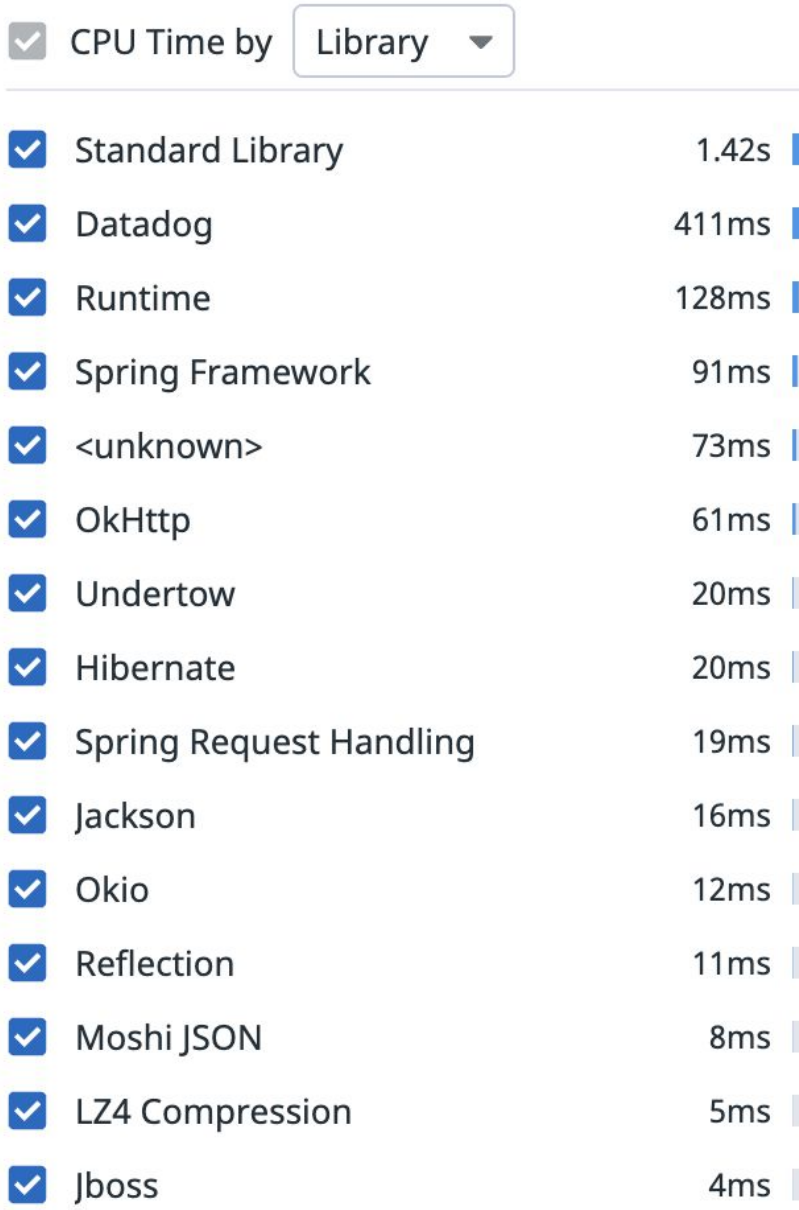
Pentesting x Observability: code insights

Demo

Pentesting x Observability: Code Insights

See what libraries are actually running, and in which paths.





DATADOG

Who can use this?

Red teams

- leverage existing internal observability products
- discover blind spots - what's not monitored is the perfect place to build persistence

Pentesters: open box testing

- ask access to customers
- great support to better understand an architecture

Pentesters: closed box testing

- stealing an access to an observability tool is **very** interesting :)

And what is coming/could come next?

Link profiles to traces and then to URLs

Get information about vulnerable libraries

Vulnerability detection

Source code integration

Open source alternatives

Open Telemetry

Prometheus

Elastic

Resources and links

Questions?

https://aviat.github.io/2022-bsideslisbon.html

Datadog is hiring! In remote, Lisbon, Paris, NYC, San Francisco…
https://securitylabs.datadoghq.com/#work-with-us