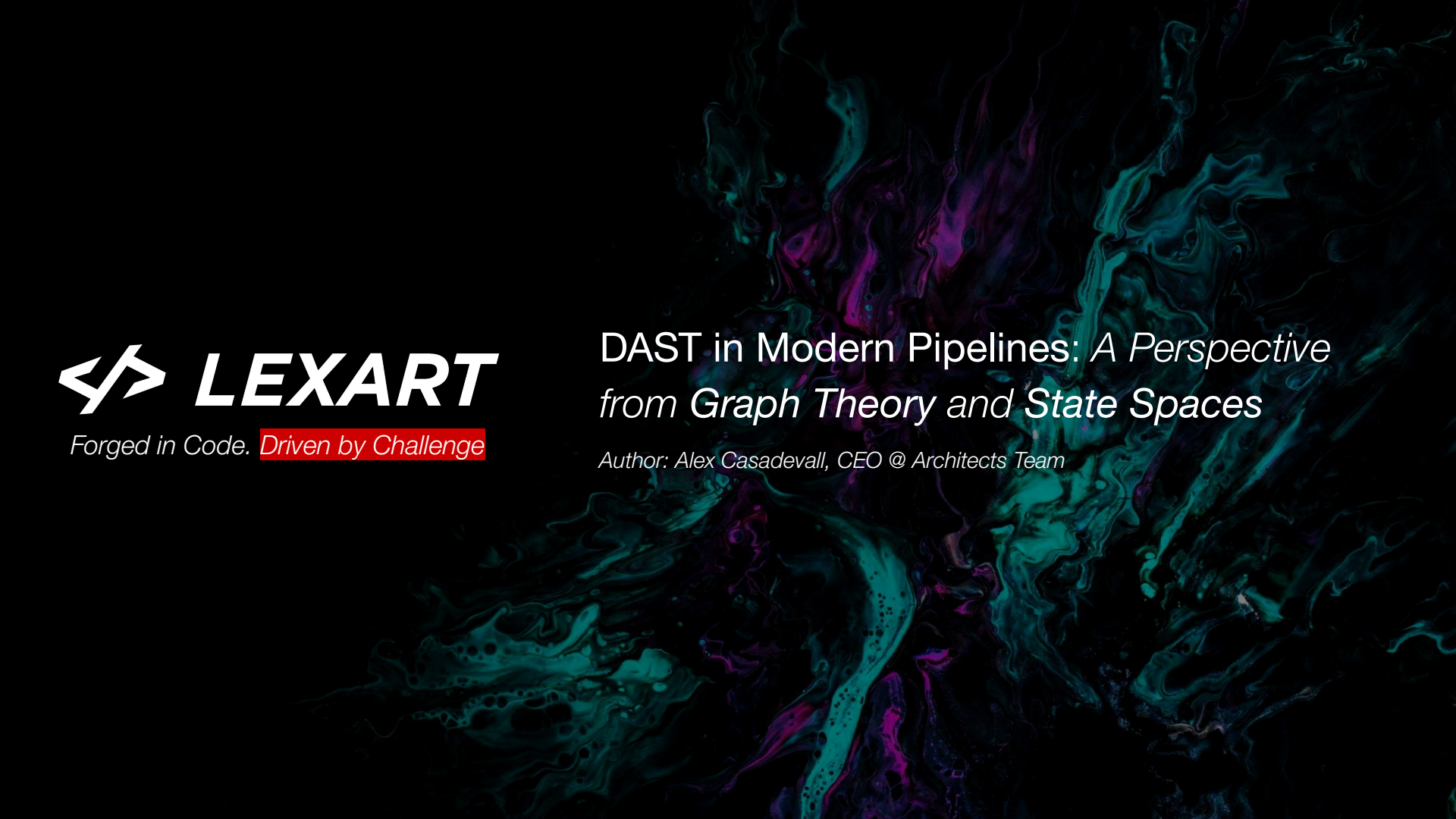
LEXART
Forged in Code. Driven by Challenge
DAST in Modern Pipelines: A Perspective from Graph Theory and State Spaces
Author: Alex Casadevall, CEO @ Architects Team

Introduction

LEXART

In practice, running a DAST (for example, OWASP ZAP) in a pipeline is usually interpreted as:

“The application was scanned and no critical vulnerabilities were detected.”

From a formal point of view, this statement is not justified. What actually happened was:

“A non-characterized fraction of the system’s possible behavior was explored.”

The difference between these two statements is structural, not semantic.

Formal Modeling of a Modern Application

LEXART

We define a directed graph:

$$G = (V, E)$$

Where:

- V: the set of observable states of the system
- E: the possible transitions between states (requests, events, callbacks)

An HTTP endpoint is not a node, but a state transition function.

States, Not URLs

LEXART

A state $s \in V$ can be represented as: $s = (u, r, t, f)$

Where:

- u: authenticated user
- r: role or permissions
- t: token / session
- f: internal system flags

Two identical requests to the same URL do not belong to the same node if any of these parameters differ.

DAST as a Graph Exploration Problem

LEXART

Formally, a DAST implements a function: $scan : G \to G'$

Where:

- G: the real graph of the system
- G': the explored subgraph

There is no guarantee that:

- G' is connected
- G' contains critical nodes
- $G' \approx G$ in structural terms

Coverage Is Not Security

LEXART

The true notion of coverage would be: $\text{coverage} = \frac{|V'|}{|V|}$

But:

- $|V|$ is unknown
- $|V|$ grows exponentially
- $|V'|$is small and biased

Therefore, coverage is not measurable in absolute terms.

NP Nature of the Problem

LEXART

Fully exploring the graph implies:

- Visiting all reachable nodes
- Under finite time constraints

This reduces to a problem of:

- Exhaustive state exploration
- With a high branching factor

In practice, it is **NP-hard due to combinatorial explosion**, even though it is not formally reducible to SAT.

Information Maximization

LEXART

Instead of “crawl everything,” prioritize nodes with:

- higher degree
- higher centrality
- higher transition fan-out

This is equivalent to:

- maximizing information gain per request

Implications for CI/CD

LEXART

What does “DAST passed” actually mean?

Formally, it only means: *“No vulnerabilities were found in the explored subgraph under these initial conditions.”*

A mature pipeline does not ask: “Did DAST pass?”

It asks instead:

- “Which region of the state space did we cover?”
- “Which assumptions did we make explicit?”

Conclusion

LEXART

DAST in modern systems is not a tool. It is a mathematical problem of partial exploration.

When it is understood this way:

- the illusion of total coverage disappears
- conscious decisions emerge
- security stops being ritual and becomes engineering