Testability Pattern-driven Web Application Security and Privacy Testing

Presented by:
Soheil Khodayari & Lukas Seidel

OBO. TESTABLE Consortium

Problem Statement

TESTABLE

- Web vulnerabilities have critical consequences for the society
  - Over 4.8 billion websites online, 1.7 billion users [1]
    - Personal data leaks, financial loss, …

Banking


Shopping


Education

- The complexity of web applications are rising

Problem: existing approaches fall short of capturing this ever-increasing complexity

- TESTABLE addresses the grand challenge of:

> Building and maintaining modern web-based and AI-powered systems **secure** and **privacy-friendly**

[1] internetlivestats.com

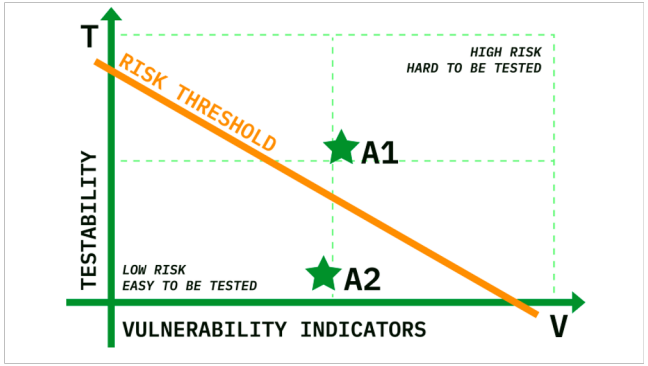
Our Vision

TESTABLE

I. New Testability Metric

- Existing methodologies for measuring the probability that a web application contains risky behaviors rely on indicators:
  - Code size/complexity, presence of sensitive function calls, …

Lowering indicators is challenging, costly, not always necessary, or even impossible!



- TESTABLE proposes a **precise risk score metric:**
  - New **bi-dimensional** metric with the novel notion of webapps' **testability** w.r.t. testing techniques
  - Compute testability via **measurable** and (possibly) **transformable testability patterns**

Our Vision (Cont'd)

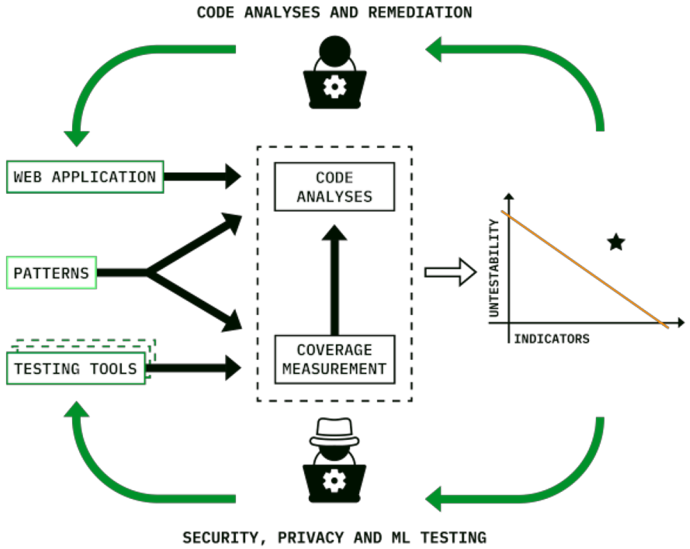
TESTABLE

I. New Testability Metric

II. New Decision and Action Space

The new testability metric provides a **natural way to improve the security and privacy** of webapps:

- **Optimize testing** by focusing on problematic components
- **Refractor design and code** to increase code testability
- **Defense in-depth layers** when no other actions are viable



Our Vision (Cont'd)

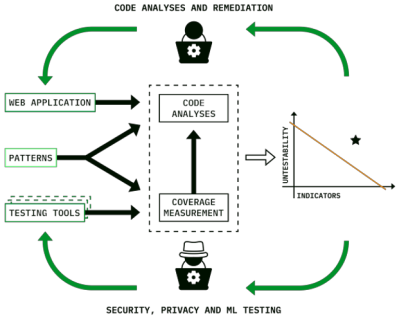
TESTABLE

I. New Testability Metric

II. New Decision and Action Space

III. New Comprehensive and Effective Testing Techniques

- Existing techniques focus on security, privacy issues often overlooked
- Reduced effectiveness due to rapid integration of ML components in webapps



Testable Domain Areas:

- **Security:** improve **security testing techniques** (SAST, DAST, and HAST)
- **Privacy:** design novel techniques to test for **privacy-related problems**
- **ML:** develop new techniques to enable **security and privacy testing of AI/ML** modules

Target Users and Policy Benefits

TESTABLE

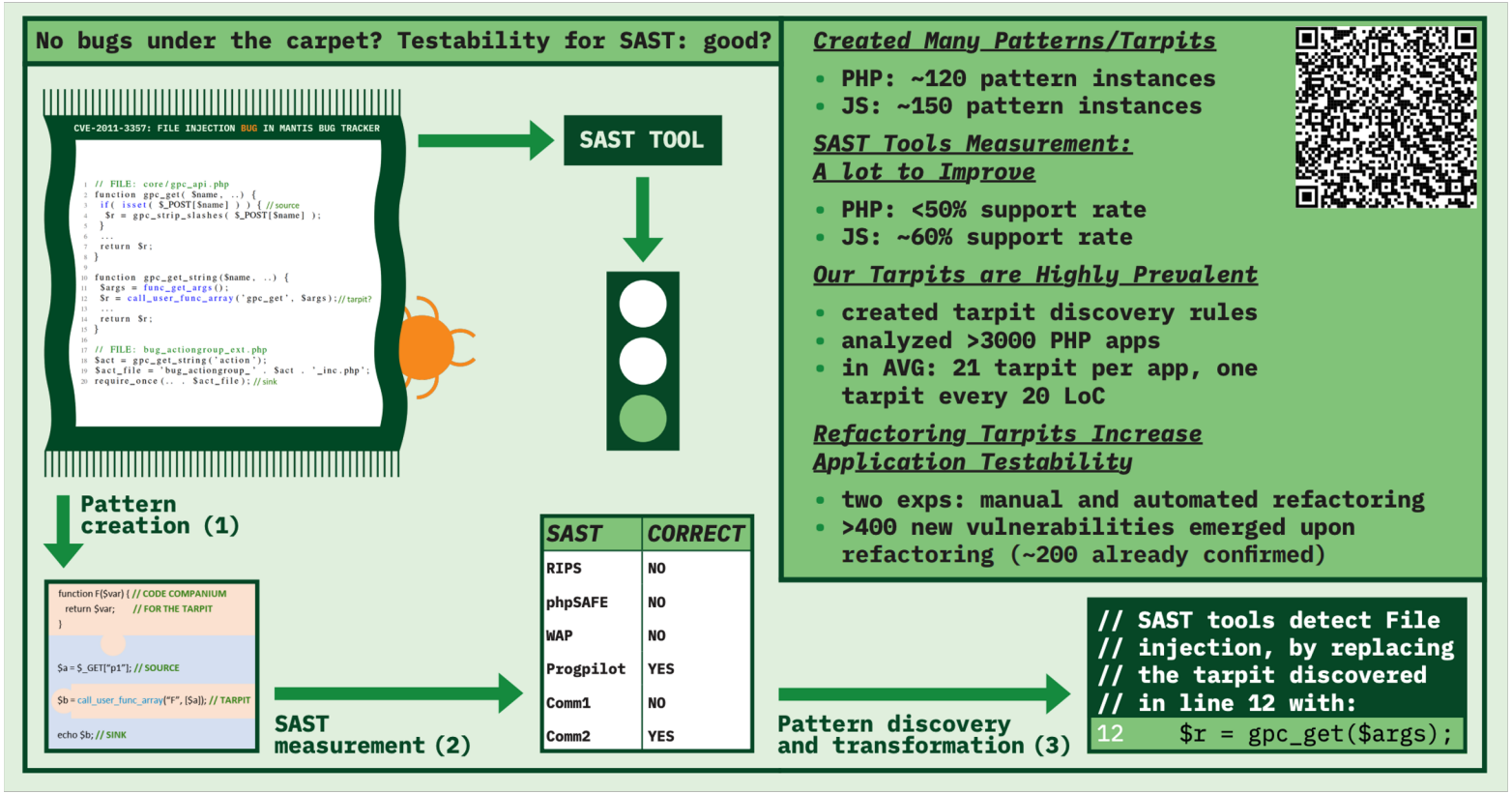
Product Managers
More precise risk estimate quantifying the security and privacy risks of a program

Product Developers
Better and flexible tools to improve testability, reducing security and privacy **risk exposure**

Security Teams
More **accurate and effective** security, privacy, and AI/ML **testing techniques** and tools

Standardization Bodies
Collection of **testability patterns and best practices** for de-facto standards

TESTABLE Over SAST: A First Story



Project Events & Dissemination

TESTABLE

- Organisation of webinar series, invited talks and seminars
- Dissemination in large internal events of the industrial project partners (SAP, NortonLifeLock)
- Participation in the organization of scientific events (conferences, workshops)
- Participation in OWASP events, and large cybersecurity conferences (e.g., BlackHat, DEFCON, etc)
- Liaison with SPARTA and Concordia competence networks
- TESTABLE open source framework (hosted by OWASP)
- TESTABLE results integrated in industrial products and development processes (Minded Security)