Web Platform Threats:

Automated Detection of Web Security Issues With WPT

Pedro **Bernardo**[1]

@bl4ck_pwn

pedro.bernardo@tuwien.ac.at

Shared first authorship with:

Lorenzo **Veronese**[1]

@310wert

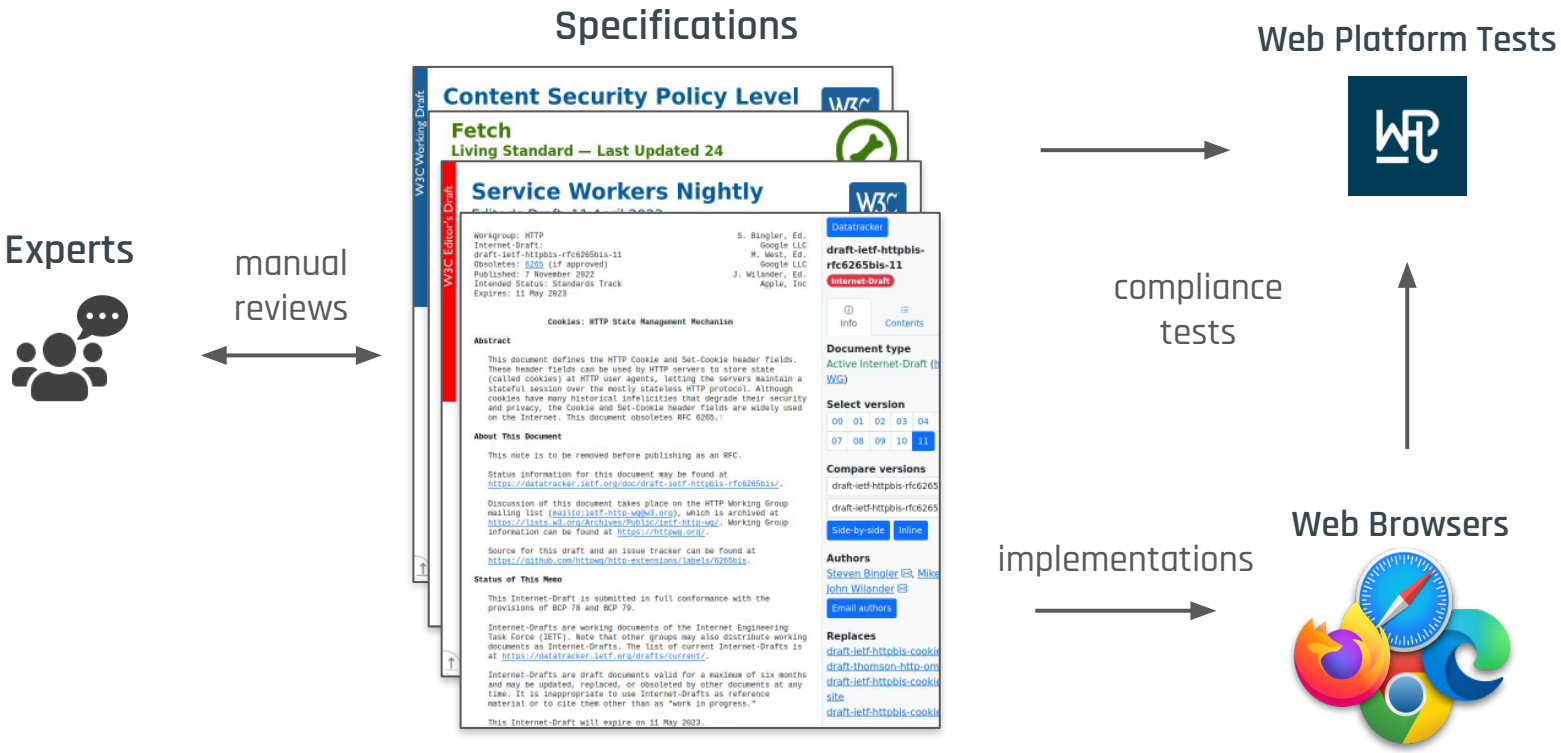
lorenzo.veronese@tuwien.ac.at

With: Valentino **Dalla Valle**[2] , Stefano **Calzavara**[2]
Marco **Squarcina**[1], Pedro **Adão**[3], Matteo **Maffei**[1]

[1] TU Wien [2] Università Ca' Foscari Venezia [3] IST, Universidade de Lisboa

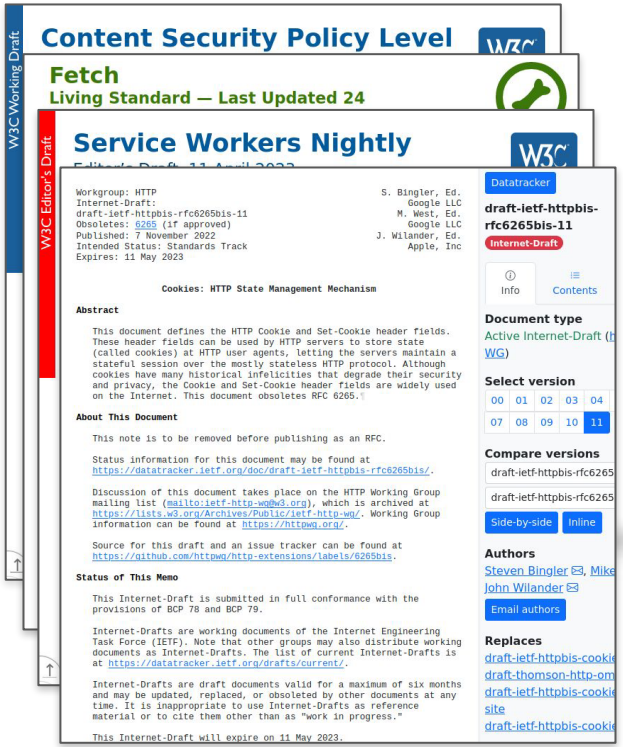
August 14–16, 2024 // Philadelphia, PA, USA

The Web Platform



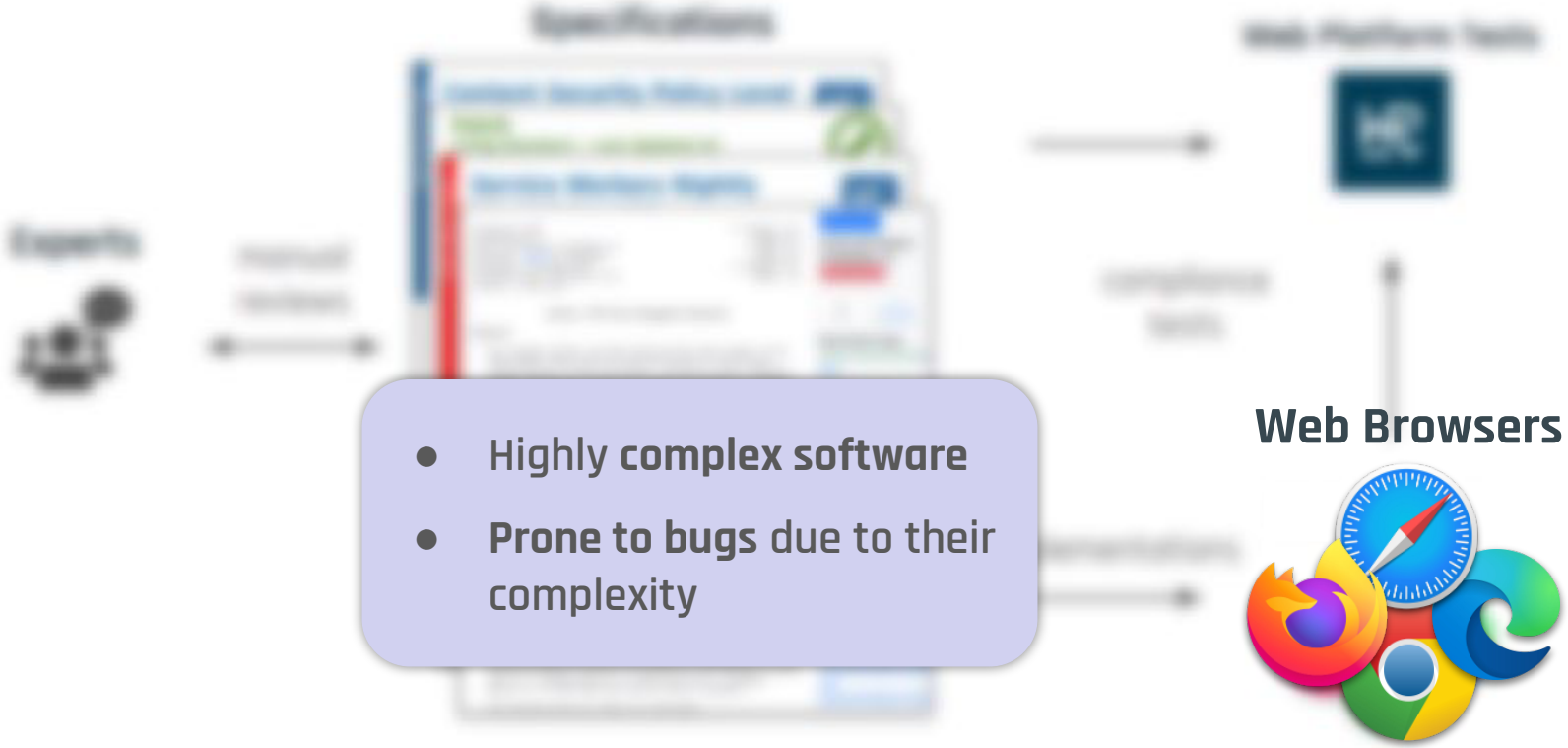
The Web Platform

Specifications



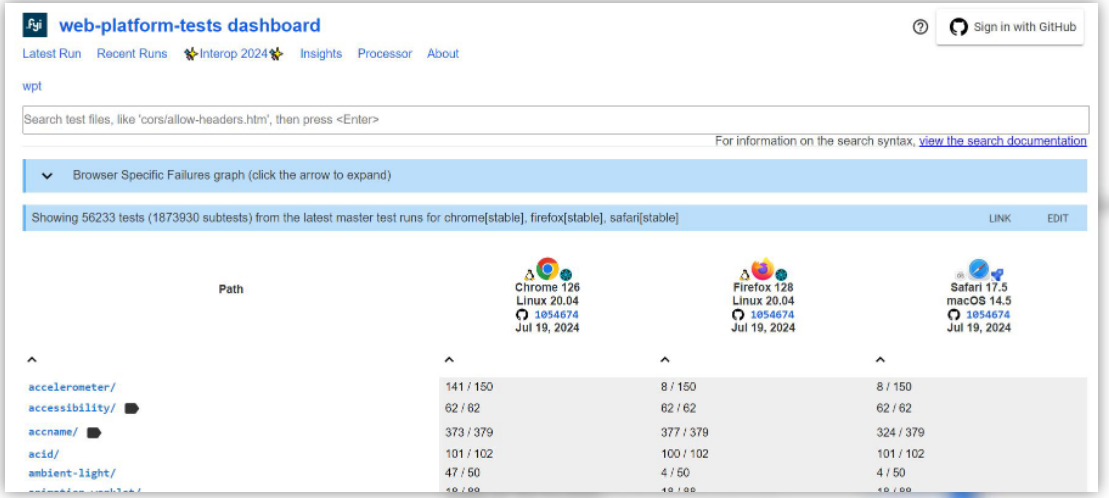
- Written **informally** in **natural language**
- **Unintended interactions** lead to **security issues**

The Web Platform



- Highly **complex software**
- **Prone to bugs** due to their complexity

The Web Platform



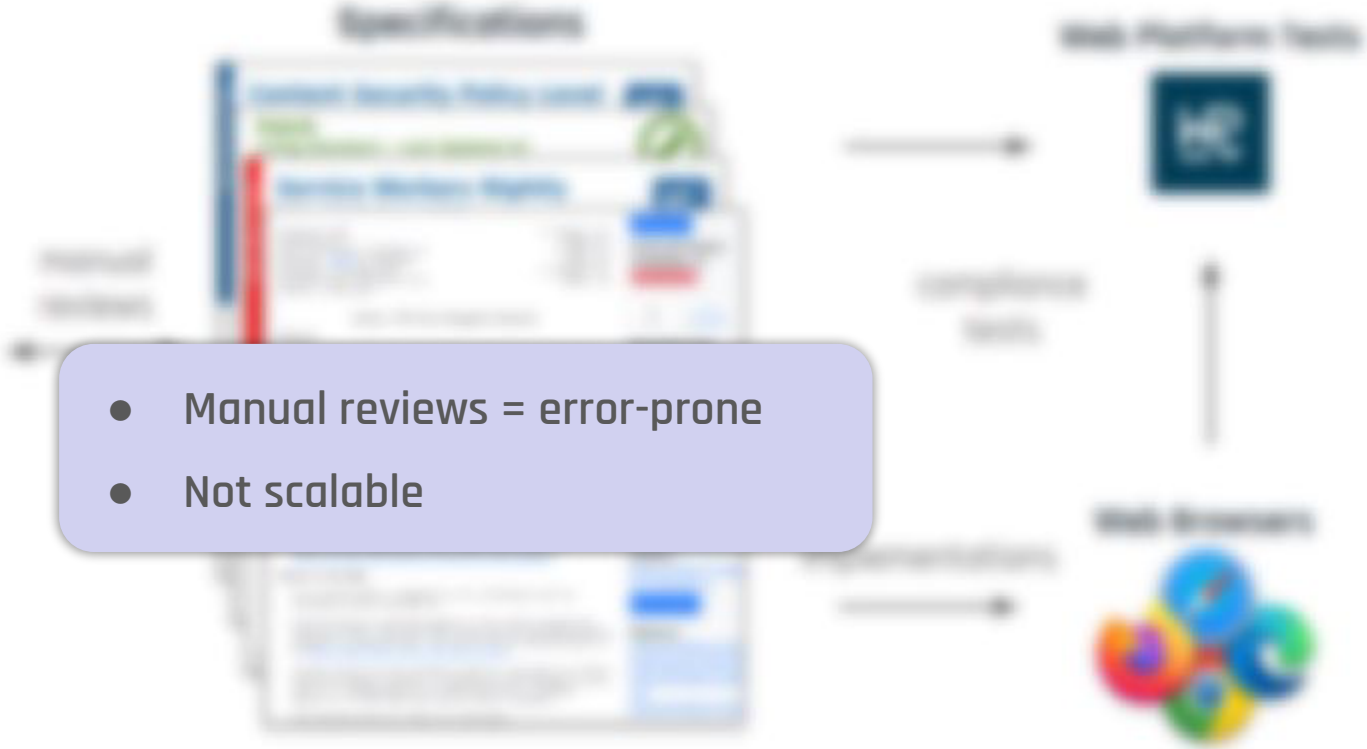
Web Platform Test

x-frame-options/	153 / 153
xhr/	2073 / 2203
Subtest Total	1829454 / 1898205

Does not reason about security

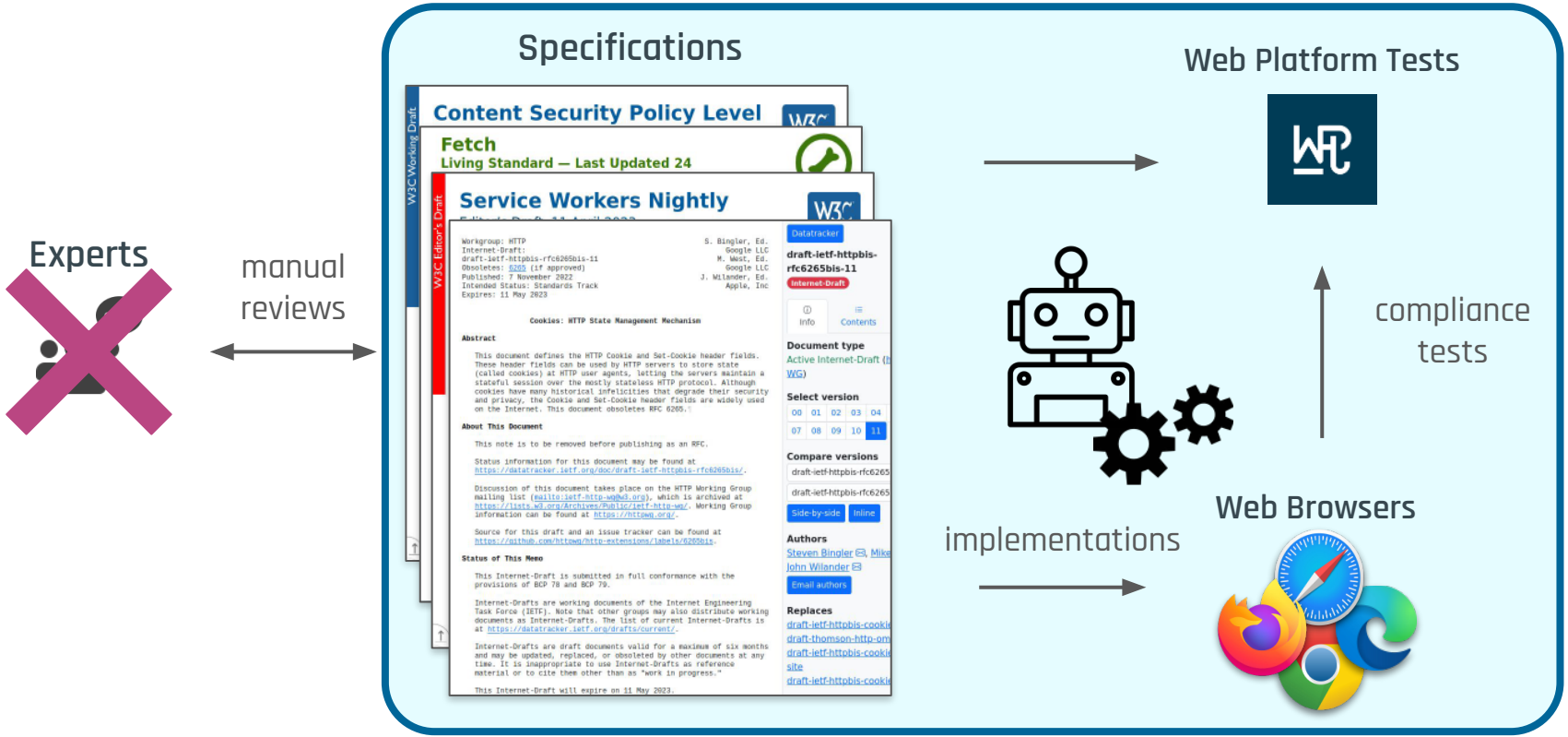
The Web Platform

Experts



- Manual reviews = error-prone
- Not scalable

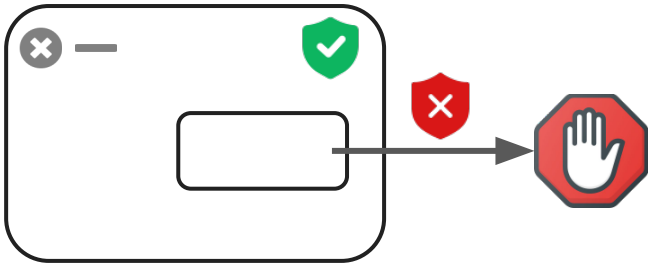
Can we automate security testing?



Web Invariants

Intended security properties of the Web that are always expected to hold

Web Invariant - Blockable Mixed Content Filtering



Insecure (http) resources fetched from **secure** (https) pages should be **blocked**

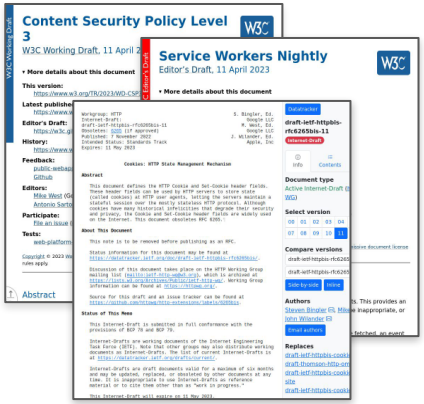
Web Invariants

Intended security properties of the Web that are always expected to hold

IEEE S&P 2023

WebSpec: Towards Machine-Checked Analysis of Browser Security Mechanisms

Lorenzo Veronese*, Benjamin Farinier†‡, Pedro Bernardo*, Mauro Tempesta*, Marco Squarcina*, Matteo Maffei*
*TU Wien
†Univ Rennes, Inria, CNRS, IRISA



Specifications

Implementations

Web Platform Threats: Overview

Web Invariants

Cookies

Mixed Content

Web Platform Threats: Overview

Web Invariants

Cookies

Mixed Content

Instrumented Browsers

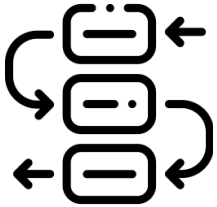
Web Platform Threats: Overview

Web Invariants

Cookies

Mixed Content

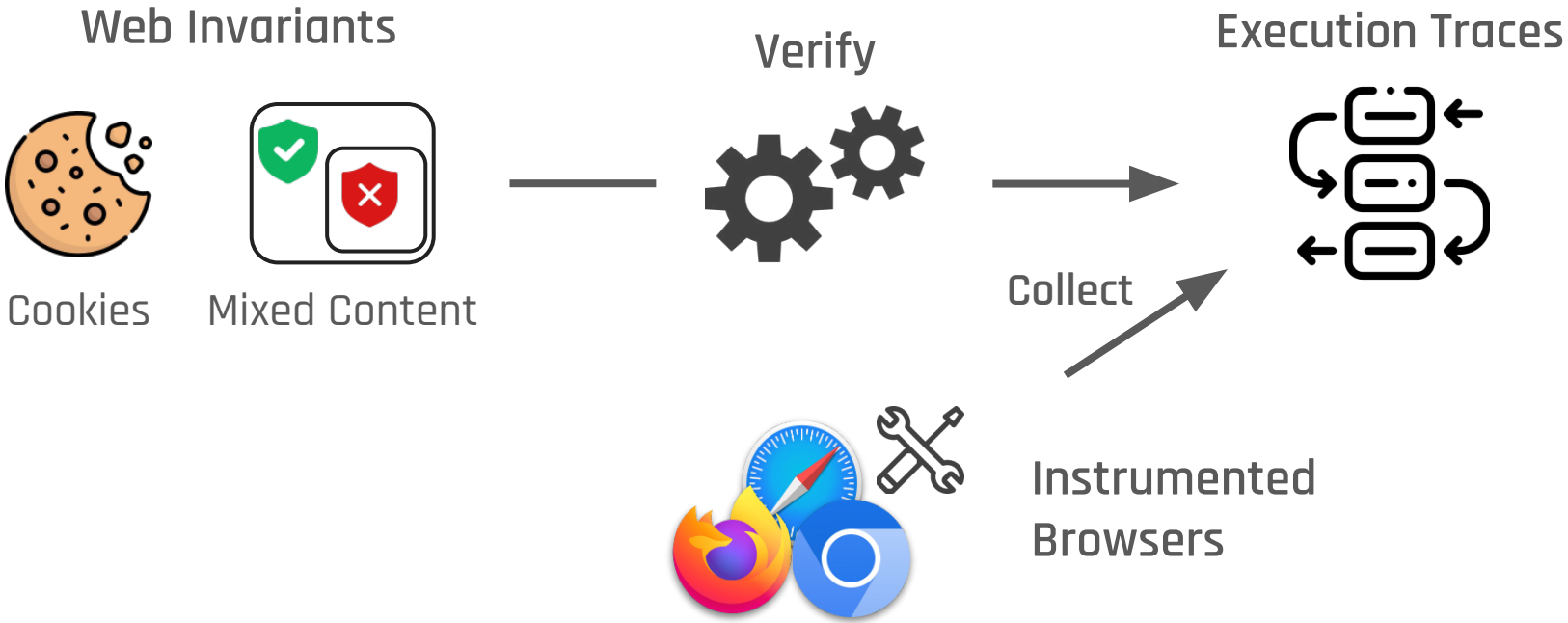
Execution Traces



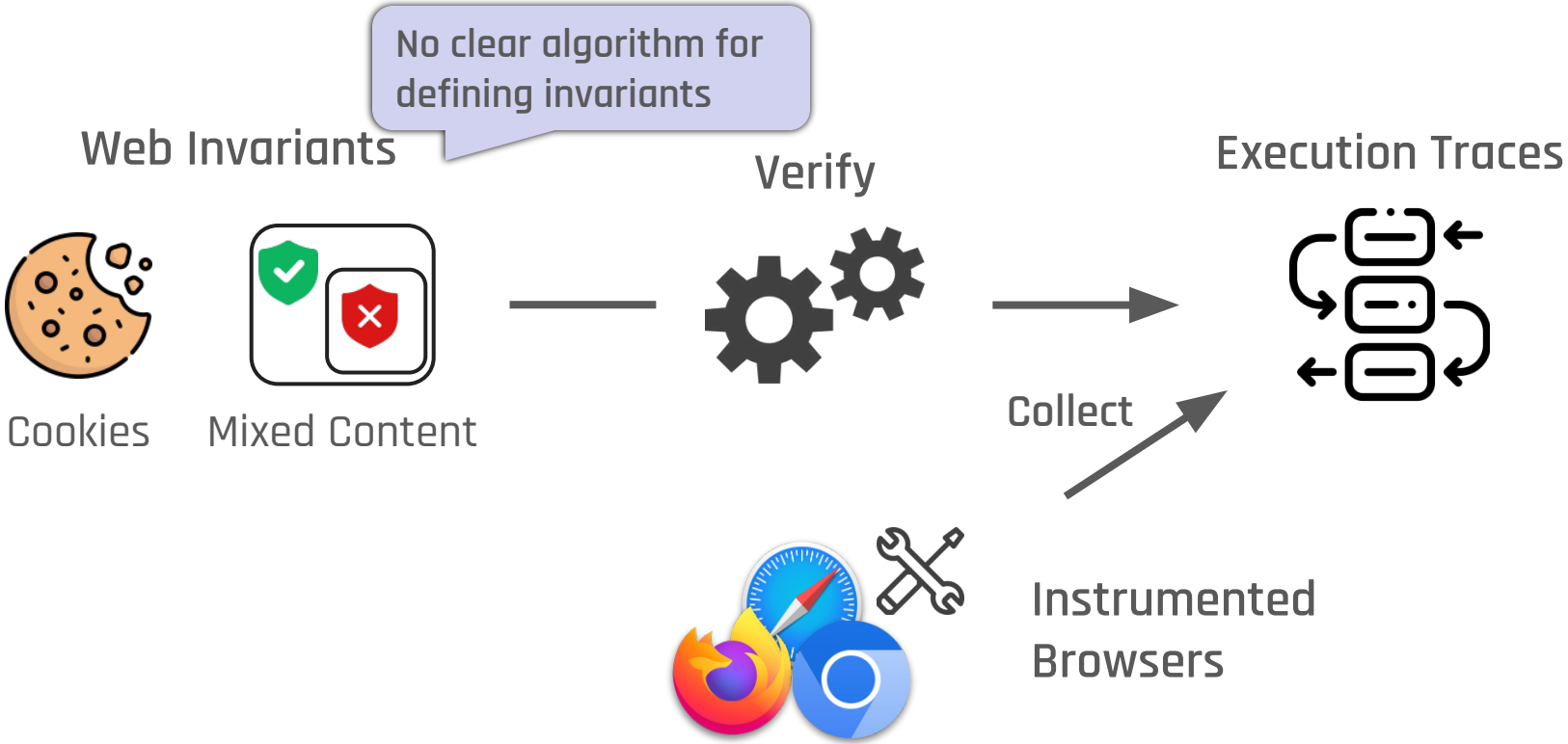
Collect

Instrumented Browsers

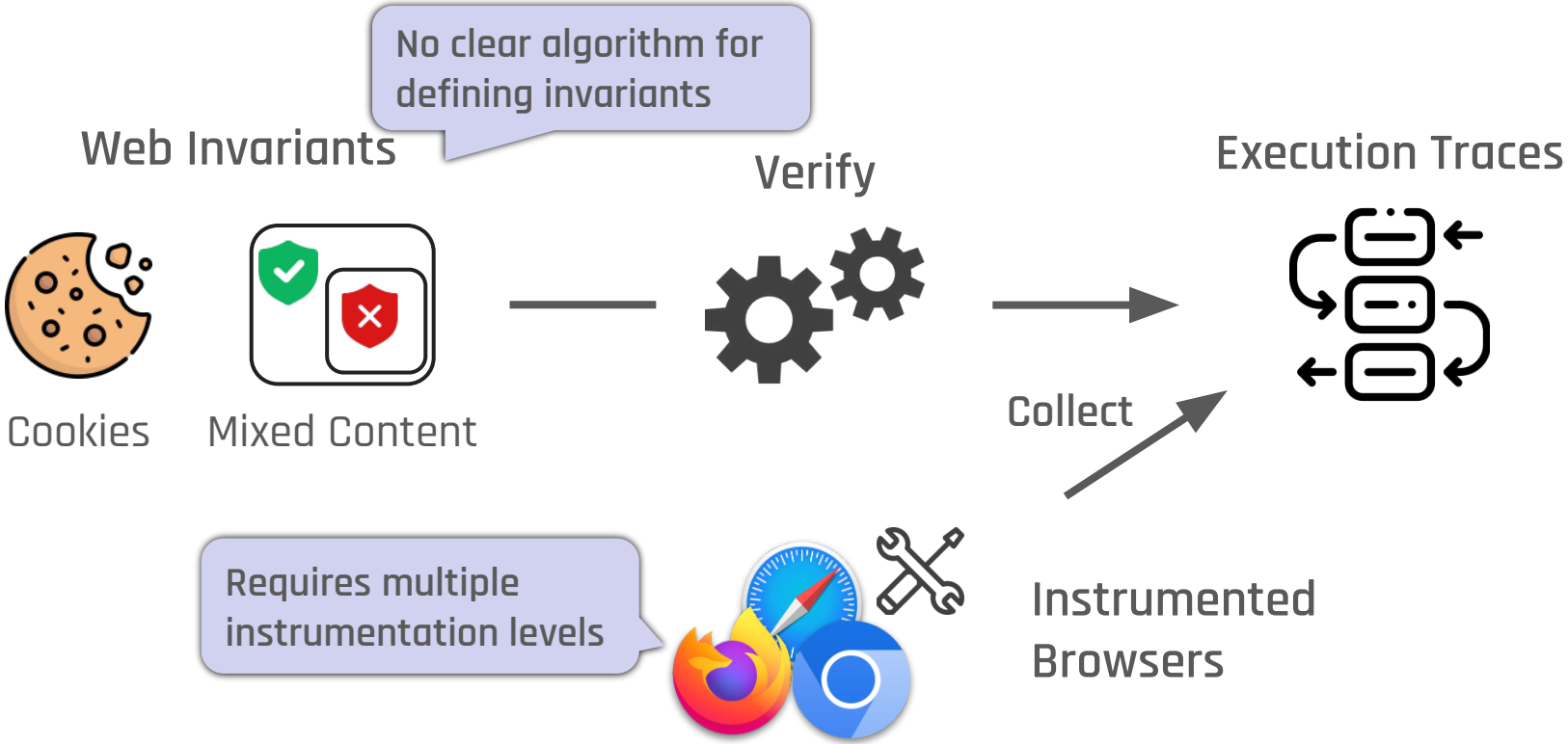
Web Platform Threats: Overview



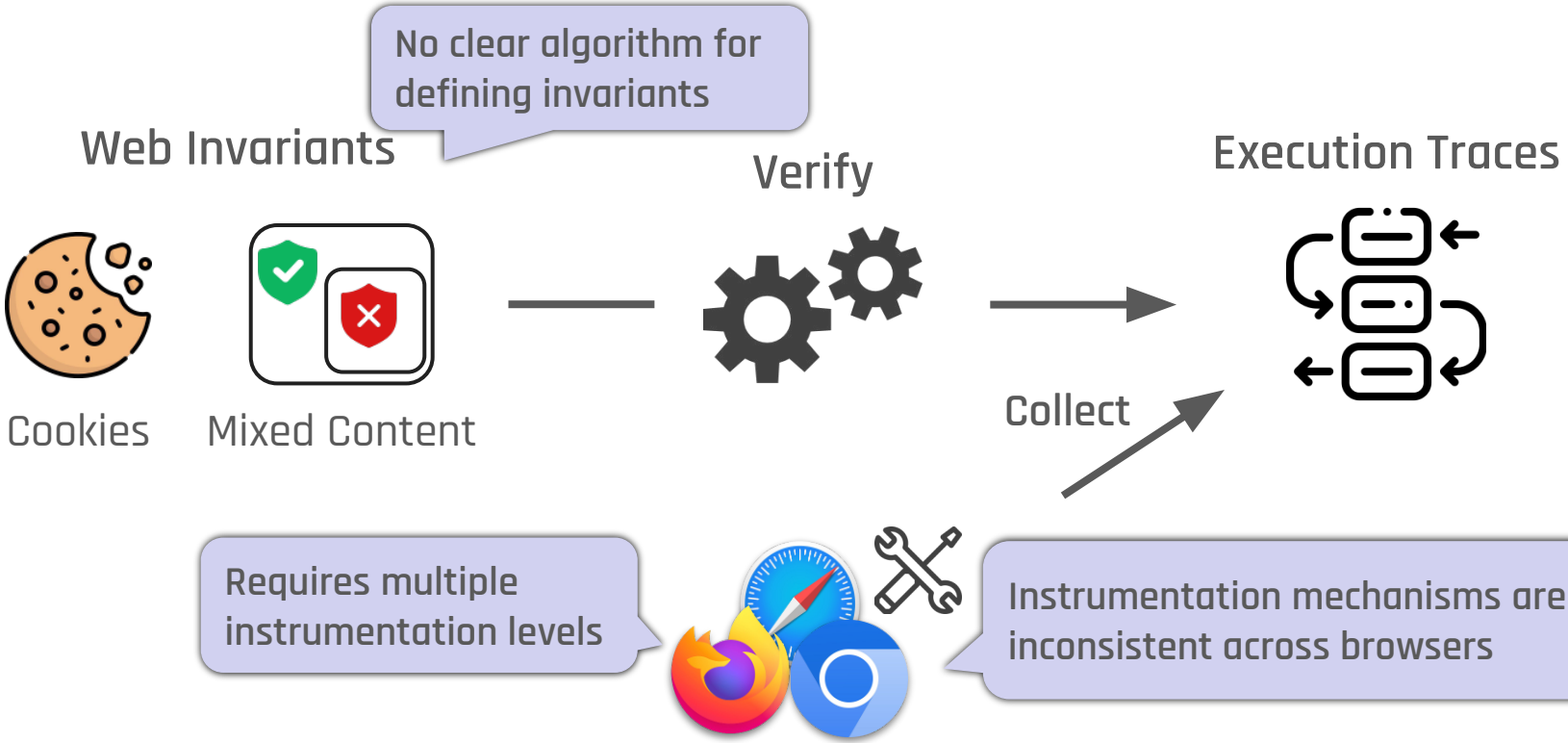
Web Platform Threats: Challenges



Web Platform Threats: Challenges



Web Platform Threats: Challenges



Web Platform Threats: Challenges

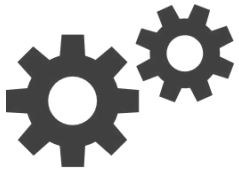
No clear algorithm for defining invariants

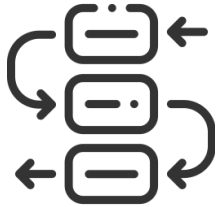
Achieving high coverage is hard

Web Invariants

Verify

Execution Traces





Cookies

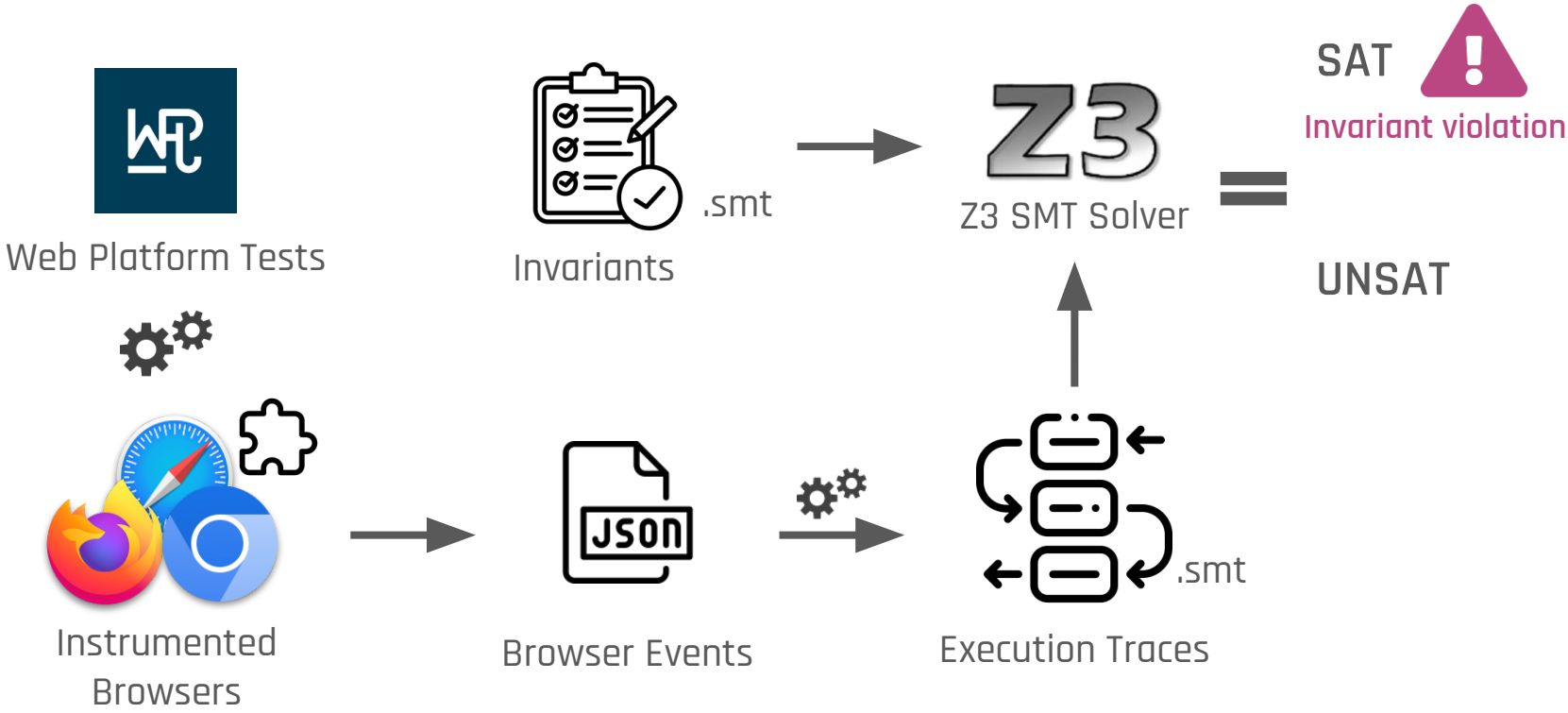
Mixed Content

Collect

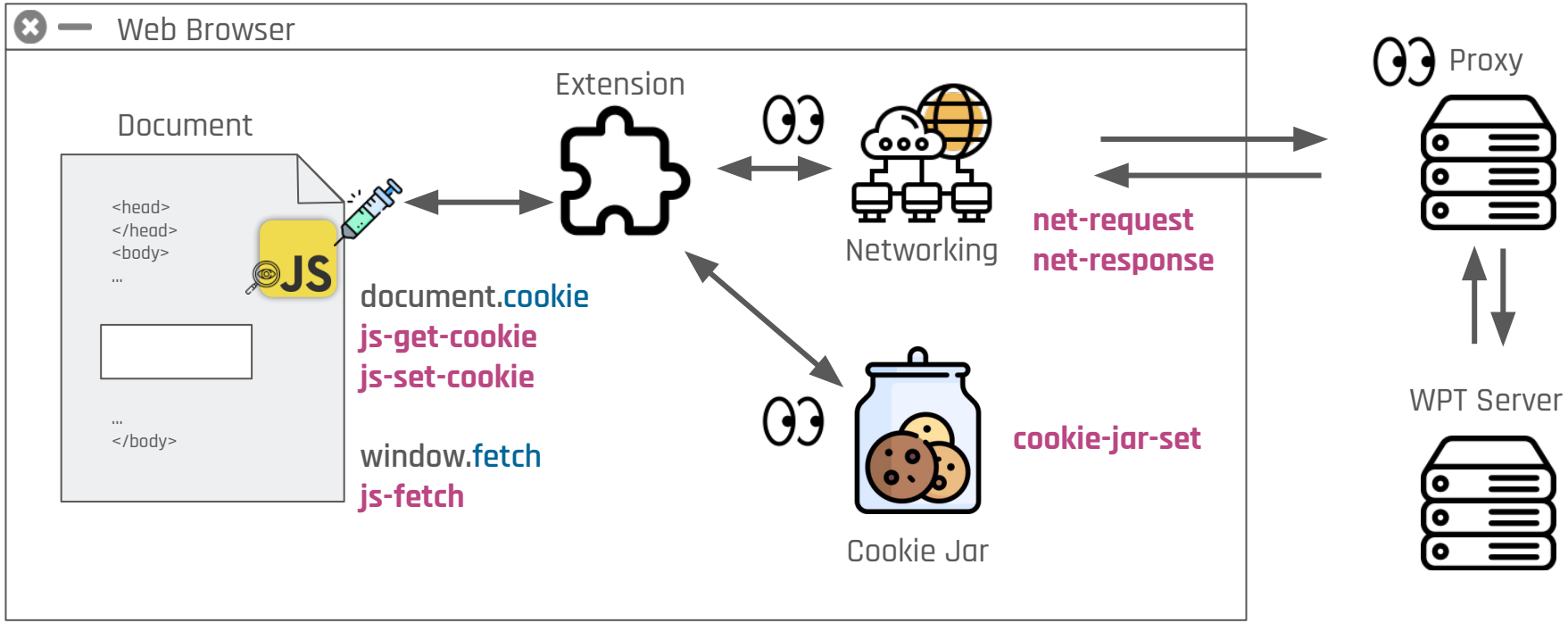
Requires multiple instrumentation levels

Instrumentation mechanisms are inconsistent across browsers

Web Platform Threats: Pipeline



Browser Instrumentation and Events

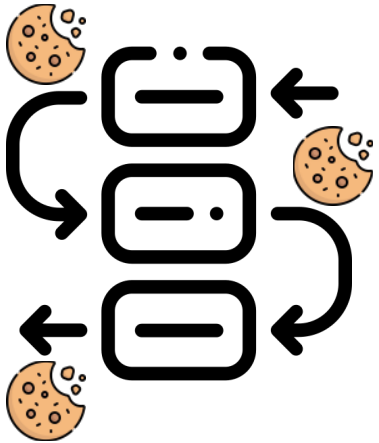


Execution Traces

Code

https://domain/path/test.html

```
test () {
  document.cookie = "A=B; secure; path=/";
  assert document.cookie.includes("A=B")
}
```



Execution Trace

t1@ js-set-cookie(**Ctx**, *"A=B; secure; path=/"*)
t2@ cookie-jar-set(*"A"*,*"B"*, secure=true,_, _, path=*"/"*, domain=*"domain"*))
t3@ js-get-cookie(**Ctx**, *"A=B"*)

Ctx = < ID, **"https://domain/path/test.html"** >

Results

Cookies

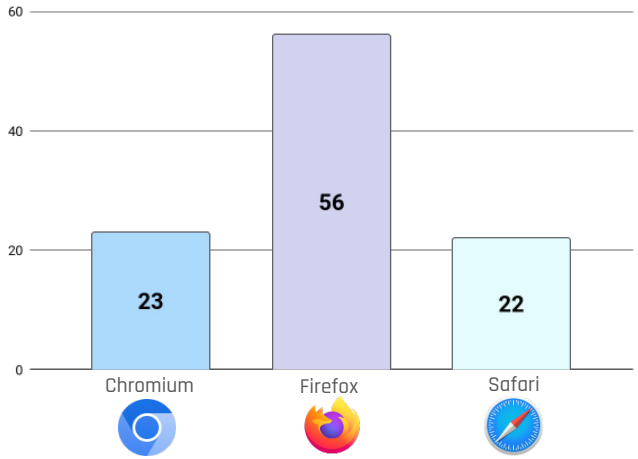
Mixed Content

	Valid
I.1 Integrity of `Secure` cookies [1]	✅
I.2 Confidentiality of `HttpOnly` cookies [1]	✅
I.3 Integrity of `__Host-` Cookies [1]	✅
I.4 Integrity of `SameSite` cookies	❌
I.5 Isolation of `SameSite` cookies	❌
I.6 Cookie serialization collision resistance	❌
I.7 Confidentiality of `Secure` cookies	✅
I.8 Blockable mixed content filtering	❌
I.9 Upgradeable mixed content filtering	❌

[1] "WebSpec: Towards Machine-Checked Analysis of Browser Security Mechanisms" 2023 IEEE S&P L. Veronese, et. al

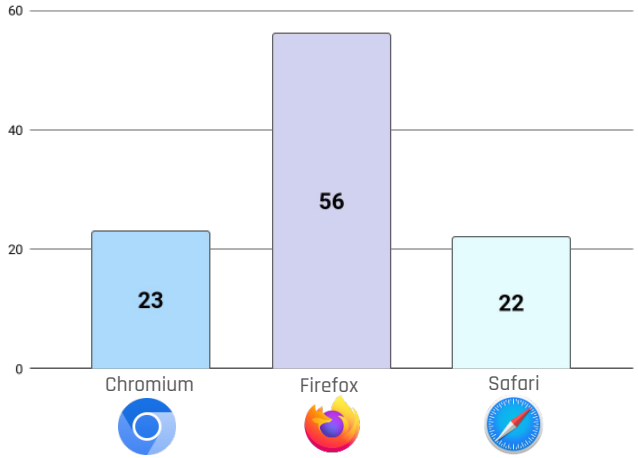
Results

- **101 Invariant violations**
- **10 vulnerabilities**
  - 8 individual reports
  - **CVE-2023-38592**
    Mixed Content Policy bypass via framing
  - **CVE-2024-6611**
    SameSite cookie integrity violation
- **Changes to rfc6265bis**
  - Clarified security implications of SameSite cookies against XS-Leaks and CSRF
  - Include support for *potentially trustworthy origins* in "secure protocol" checks



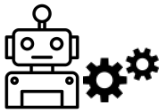
Results

- **101 Invariant violations**
- **10 vulnerabilities**
  - 8 individual reports
  - **CVE-2023-38592**
    Mixed Content Policy bypass via framing
  - **CVE-2024-6611**
    SameSite cookie integrity violation
- **Changes to rfc6265bis**
  - Clarified security implications of SameSite cookies against XS-Leaks and CSRF
  - Include support for *potentially trustworthy origins* in "secure protocol" checks



- 15 false positive traces
  - Missing events
  - Incorrectly ordered events
  - Missing information in events

Conclusion



Automated analysis can detect invariant violations during development

Limitations can be mitigated with better instrumentation support

Defining Web invariants should be a priority

Web Platform Threats:
Automated Detection of Web Security Issues With WPT

Thank you!

Pedro Bernardo

@bl4ck_pwn
pedro.bernardo@tuwien.ac.at

Icons by **flaticon**