Trust Me *If* You Can

How Usable Is Trusted Types In Practice?

Sebastian Roth, Lea Gröber, Philipp Baus, Katharina Krombholz, and Ben Stock

USENIX Security Symposium 2024
Philadelphia, PA, USA

TU WIEN

S&P Security & Privacy

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

History of Trusted Types

Explainer: Trusted Types for DOM Manipulation

– Mike West on TrustedTypes GitHub

„[…] consider this a Formal Objection“

– Mozilla on WebAppSec GitHub

Google report on their success in deploying Trusted Types

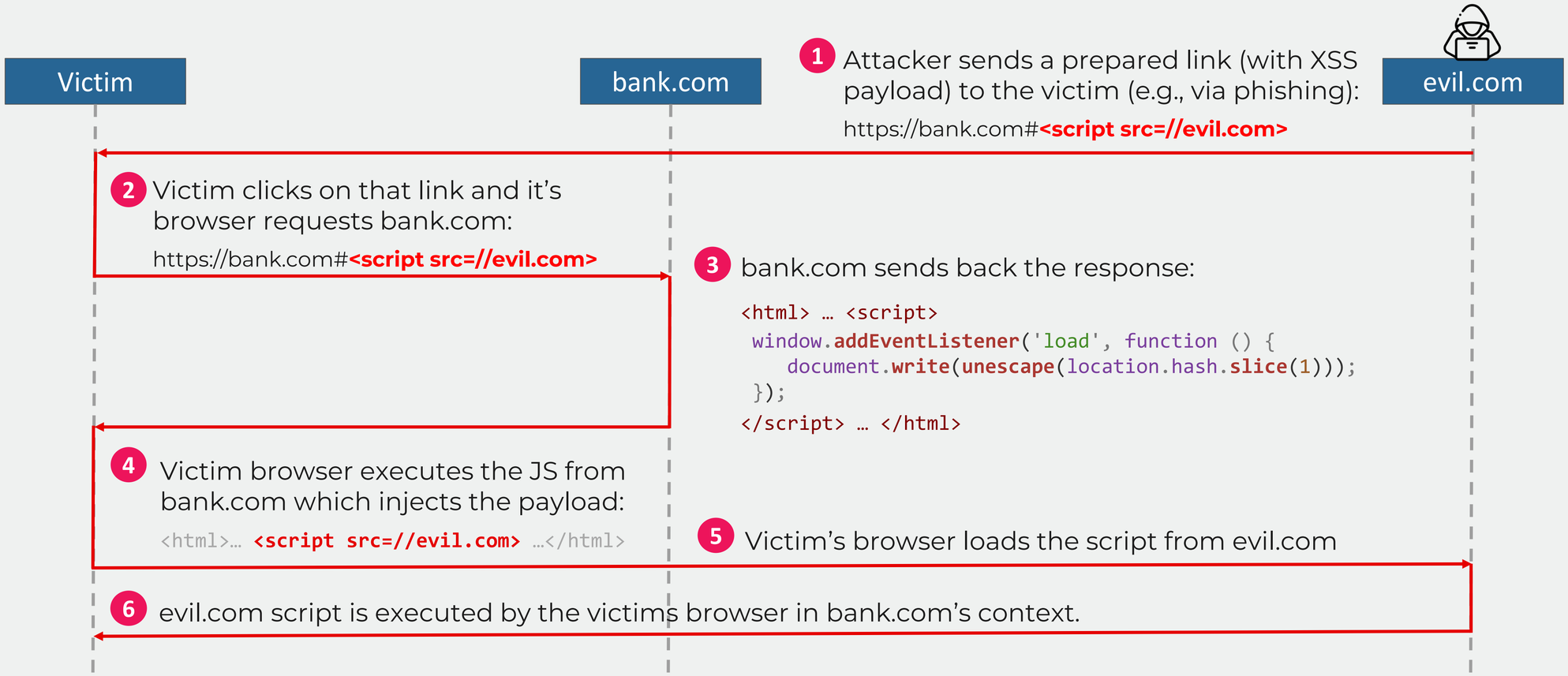
12 Angry Developers – A Qualitative Study on Developers' Struggles with CSP

– CCS 2021

„We […] intent to change our standard position to positive“

– Mozilla on WebAppSec GitHub

Client-Side Cross-Site Scripting (XSS)



What is Trusted Types?

```
Content-Security-Policy: require-trusted-types-for 'script'; trusted-types ttpolicy;
```

vulnerable.js

```
window.addEventListener('load', function () {
    let d = document.createElement('div');
    var name = unescape(location.hash.slice(1));
    d.innerHTML = ttpolicy.createHTML(name);
    document.body.appendChild(d);
});
```

trusted-types.js

```
if (window.trustedTypes && trustedTypes.createPolicy) {
    trustedTypes.createPolicy('ttpolicy', {
        createHTML: function(html_string) {
            return sanitizeHTML(html_string);
        },
        createScript: function(js_string) {
            return sanitizeJS(js_string);
        },
        createScriptUrl: function(url) {
            return checkURL(url);
        },
    });
}
```

What is Trusted Types?

```
Content-Security-Policy: require-trusted-types-for 'script'; trusted-types default;
```

vulnerable.js

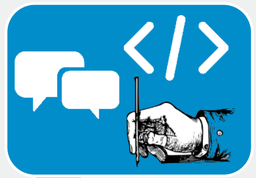
```
window.addEventListener('load', function () {
    let d = document.createElement('div');
    d.innerHTML = unescape(location.hash.slice(1));
    document.body.appendChild(d);
});

window.addEventListener('load', function () {
    eval(unescape(location.hash.slice(1)));
});

window.addEventListener('load', function () {
    let s = document.createElement('script');
    s.src = unescape(location.hash.slice(1));
    document.body.appendChild(s);
});
```

trusted-types.js

```
if (window.trustedTypes && trustedTypes.createPolicy) {
    trustedTypes.createPolicy('default', {
        createHTML: function(html_string) {
            return sanitizeHTML(html_string);
        },
        createScript: function(js_string) {
            return sanitizeJS(js_string);
        },
        createScriptUrl: function(url) {
            return checkURL(url);
        },
    });
}
```

Challenges & Methodology

Key Challenges
• Targeted Population • Coding Task Design



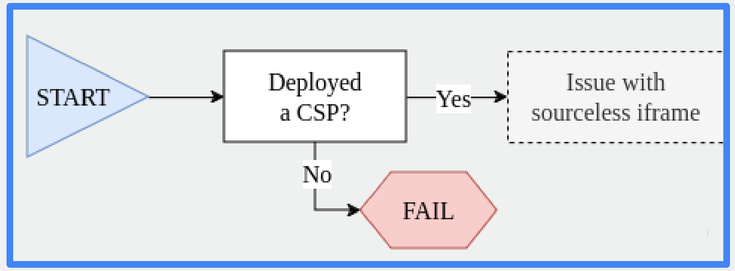
Semi-Structured Interview
Incl. Coding Task

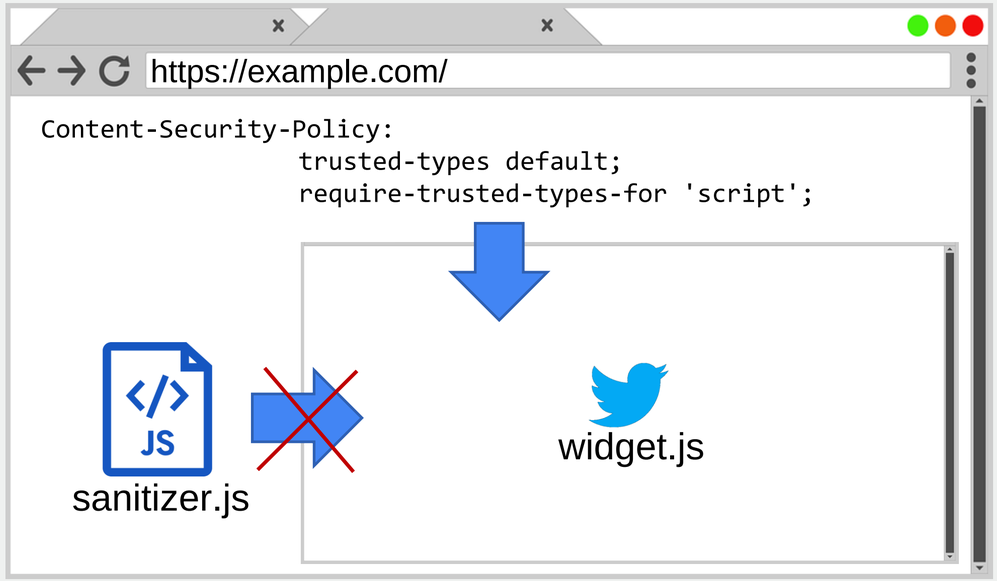
Interview Transcription

Open Coding Process

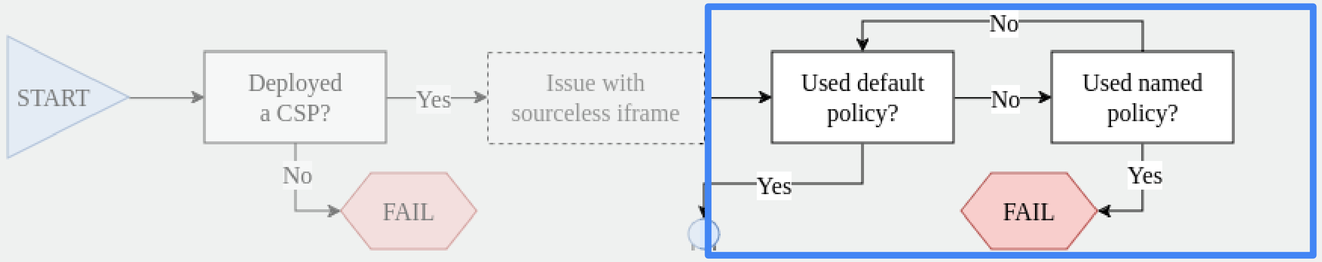
Find Deployment
Strategies and
Roadblocks of TT

Strategies & Roadblocks

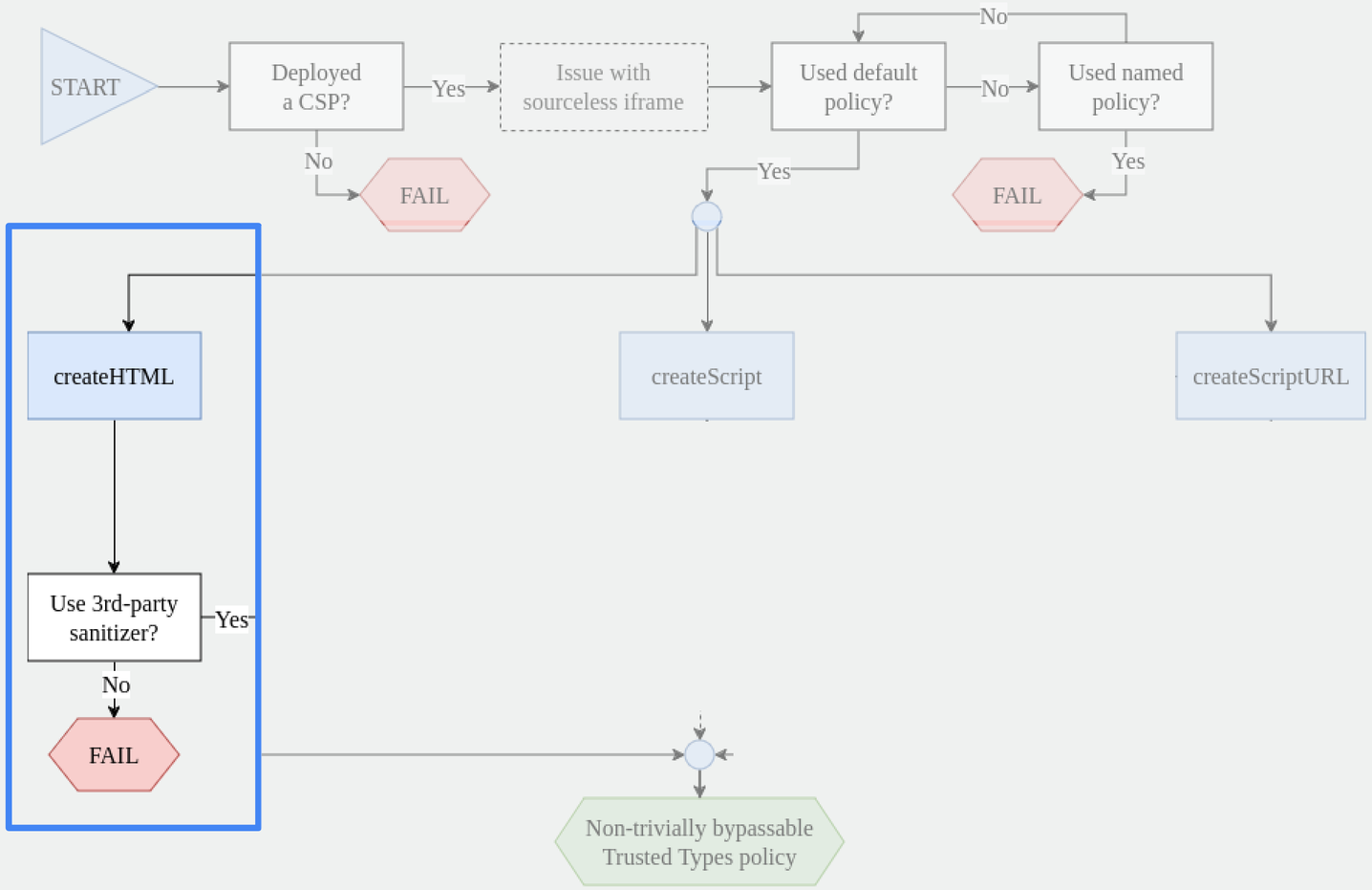




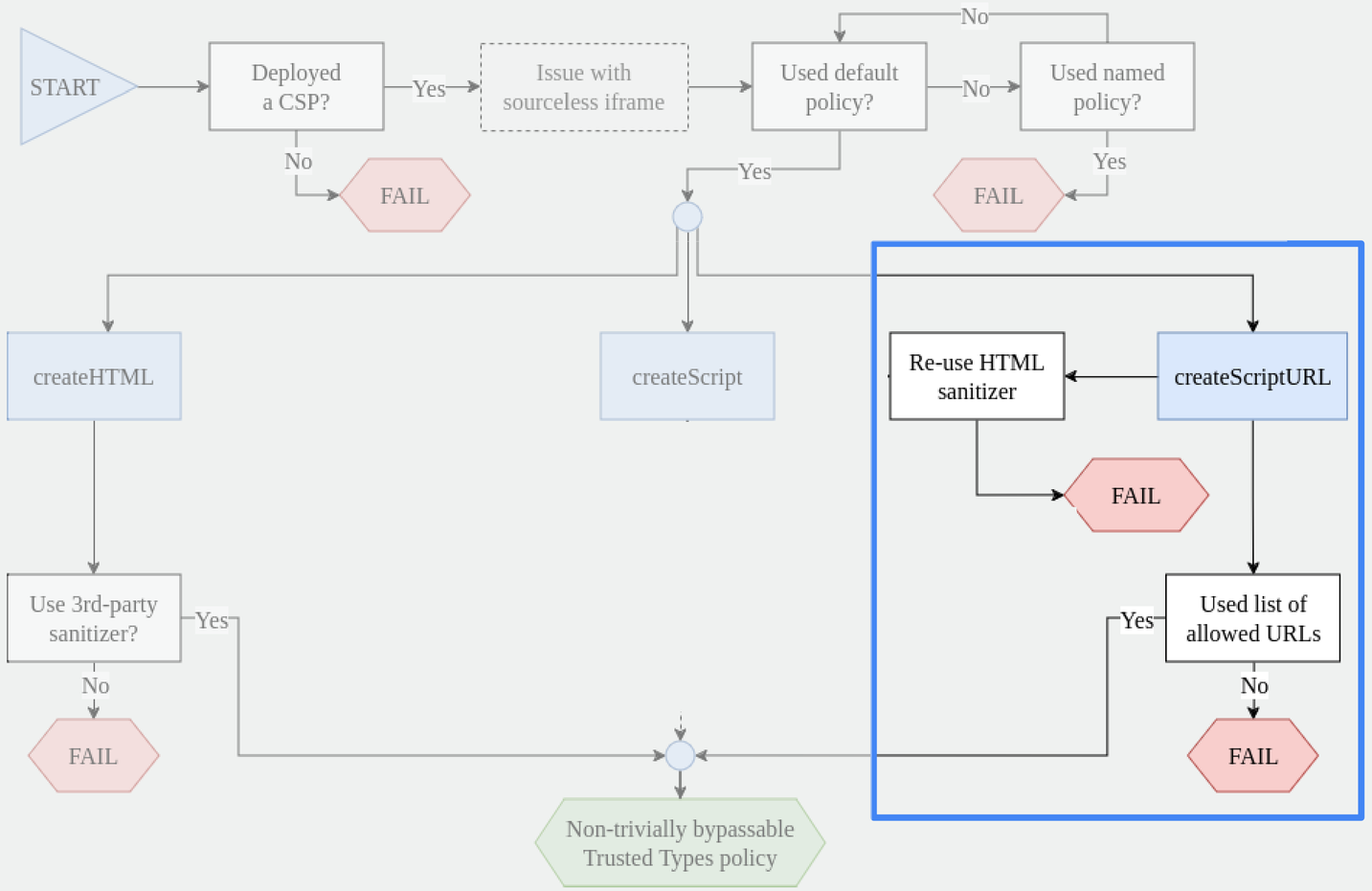
Strategies & Roadblocks



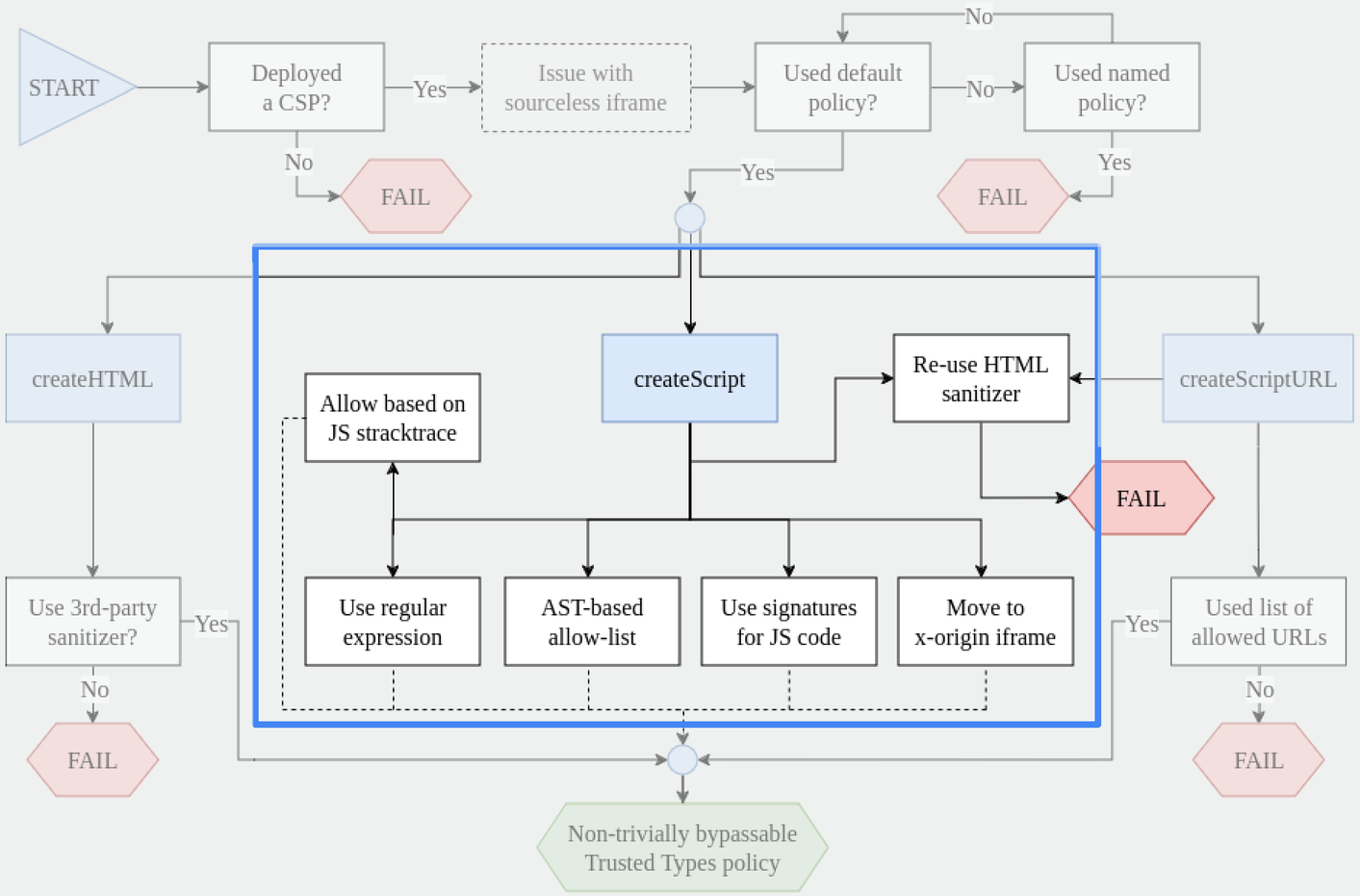
Strategies & Roadblocks



Strategies & Roadblocks



Strategies & Roadblocks



Improvement Suggestions

- Ease the implementation of the HTML sanitizer
- Fix the sourceless iframe inheritance problem

- Think about TT integration from the beginning
- Default policies ease the deployment for existing projects
- Choose third parties with care

- Improve information sources and better materials to adhere to real-world scenario
- Work on better tools and evaluate them together with developers

Summary

What is Trusted Types?

Content

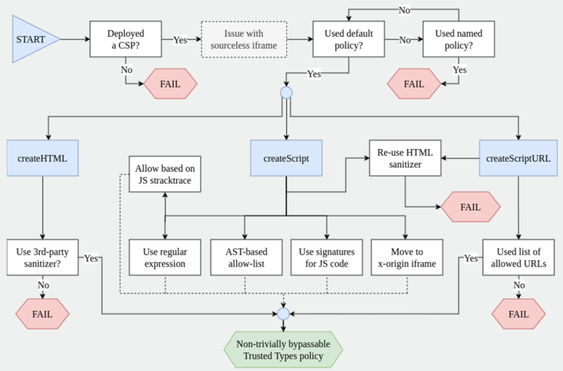
```
window.addEven
    let d = do
    d.innerHTM
    document.b
});

window.addEven
    eval(unesc
});

window.addEven
    let s = do
    s.src = un
    document.b
});
```

Challenges & Methodology

Key Chal

- Targeted Pop
- Coding Task D

Strategies & Roadblocks



Read the paper!

@s3br0th
@snroth@infosec.exchange
linkedin.com/in/snroth
github.com/rothsn
sebastian.roth@tuwien.ac.at