Integrácia knižnice Trusted Types do knižníc a frameworkov s voľne dostupným zdrojovým kódom

Emanuel Tesař

Vedúci práce: RNDr. Peter Borovanský, PhD.

Konzultant: Krzysztof Kotowicz

Úvod

- Cross site scripting (XSS) zraniteľnosť

```
<!DOCTYPE html>
<html lang="en">
  <body>
    <div id="content"></div>
    <script type="text/javascript">
      // https://example.com?<img%20src=x%20onerror="alert(1)"></img>
      const content = decodeURIComponent(location.search.substr(1))
      document.getElementById('content').innerHTML = 'URL content: ' + content
    </script>
  </body>
</html>
```

Úvod

- Knižnica Trusted Types = obmedzenie prístupu k nebezpečným funkciám

```
1   // Don't do
2   el.innerHTML = '<img src=xyz.jpg>';
3
4   // Do
5   el.textContent = '';
6   const img = document.createElement('img');
7   img.src = 'xyz.jpg';
8   el.appendChild(img);
```

Úvod

- Trusted Types policies = tvorba vlastných vierohodných typov

```
1   // Create and use policy
2   if (window.trustedTypes && trustedTypes.createPolicy) {
3     const escapeHTMLPolicy = trustedTypes.createPolicy('myEscapePolicy', {
4       createHTML: string => string.replace(/\</g, '&lt;')
5     });
6
7
8     const escaped = escapeHTMLPolicy.createHTML('<img src=x onerror=alert(1)>');
9     console.log(escaped instanceof TrustedHTML);  // true
10    el.innerHTML = escaped;  // Assignment works!
11  }
12
```

Úvod

- Tvorba moderných webových aplikácií
  - využívanie bezplatných knižníc s voľne dostupným zdrojovým kódom
  - veľké množstvo knižníc a nástrojov
- Motivácia a ciele našej práce
  - Analýza procesu integrácie
  - Integrácia a analýza Trusted Types integrácií

Proces integrácie

- Založený na našich skúsenostiach
- Zoznamovanie sa s projektom
- 3 fázy
    a. Hľadanie nebezpečných funkcií
    b. Hľadanie alternatívnych riešení
    c. Implementácia integrácie

Preprocesory kódu

- Kompilátory, bundlery a transformátory
- Naše kontribúcie
  a. JSX transformátor pre knižnicu Solid.js
  b. Vite bundler
  c. Webpack-dev-server (dokončený až po odovzdaní práce)

JSX transformátor pre knižnicu Solid.js

```jsx
import { render } from "solid-js/web";
import { createSignal } from "solid-js";

function Counter() {
  const [count, setCount] = createSignal(0);
  const increment = () => setCount(count() + 1);

  return (
    <button type="button" onClick={increment}>
      {count()}
    </button>
  );
}

render(() => <Counter />, document.getElementById("app"));
```

```jsx
import { render, createComponent, delegateEvents, insert, template } from 'solid-js
import { createSignal } from 'solid-js';

const _tmpl$ = /*#__PURE__*/template(`<button type="button"></button>`, 2);

function Counter() {
  const [count, setCount] = createSignal(0);

  const increment = () => setCount(count() + 1);

  return (() => {
    const _el$ = _tmpl$.cloneNode(true);

    _el$.$$click = increment;

    insert(_el$, count);

    return _el$;
  })();
}

render(() => createComponent(Counter, {}), document.getElementById("app"));

delegateEvents(["click"]);
```

JSX transformátor pre knižnicu Solid.js

```
39  let policy;
40  if (window.trustedTypes) {
41    policy = window.trustedTypes.createPolicy("solid-dom-expressions", {
42      createHTML: s => s
43    });
44  }
45
46  export function template(html, check, isSVG) {
47    const t = document.createElement("template");
48    t.innerHTML = policy ? policy.createHTML(html) : html;
49    let node = t.content.firstChild;
50    if (isSVG) node = node.firstChild;
51    return node;
52  }
53
```

Integrácia do webových knižníc

- Create React App (CRA)
  - Využívajúc existujúcu integráciu v knižnici React
  - Využívajúc našu Webpack-dev-server integráciu
- Solid.js
  - Využívajúc našu Vite integráciu
  - Testovanie - integračné testy, existujúca aplikácia menšieho rozsahu

Testovacie knižnice

- Implementácia testovacieho modulu pre knižnicu Cypress
- Sprístupnenie modulu pre verejnosť
- Dokumentácia
- Publikácia do správcu balíčkov npm

Zhrnutie a ďalšie plány

- Analýza a implementácia integrácií knižnice Trusted Types
  - Solid.js
  - Cypress modul
- Materiály zverejnené online na stránke Github
- Snaha znížiť riziko XSS zraniteľností vo webových aplikáciách
- Ďalšia spolupráca s pánom K. Kotowiczom
  - Zlúčenie našich integrácií do projektov Solid.js a Vite

Ďakujem.