

COMENIUS UNIVERSITY IN BRATISLAVA
FACULTY OF MATHEMATICS, PHYSICS AND INFORMATICS

TRUSTED TYPES INTEGRATION INTO OPEN
SOURCE FRAMEWORKS AND LIBRARIES
MASTERS THESIS

2021

EMANUEL TESÁŘ, BC.

COMENIUS UNIVERSITY IN BRATISLAVA
FACULTY OF MATHEMATICS, PHYSICS AND INFORMATICS

TRUSTED TYPES INTEGRATION INTO OPEN
SOURCE FRAMEWORKS AND LIBRARIES
MASTERS THESIS

Study Programme: Computer Science
Field of Study: Computer Science
Department: FMFI.KAI - Department of Applied Informatics
Supervisor: RNDr. Peter Borovanský, PhD.
Consultant: Krzysztof Kotowicz

Bratislava, 2021
Emanuel Tesař, Bc.

Acknowledgments:

Abstrakt

Klíčové slová: Trusted Types, Web APIs

Abstract

Trusted Types is a modern Web API which aims to reduce DOM XSS attack surface in web applications. They give you the tools to write and maintain applications free of DOM XSS vulnerabilities by making the dangerous web API secure by default. Currently, they are supported in Chrome, Edge and Opera.

Integrating Trusted Types in web applications and libraries requires code changes. The major problem is when these changes need to be made in third party code which you don't have access to and you can't easily modify. Trusted Types support in open source projects is gradually improving and our plan is to analyze these integrations and implement one or more of the challenging ones.

Keywords: Trusted Types, Web APIs

Contents

Concepts and definitions	1
1 Introduction	3
1.1 Cross site scripting (XSS)	3
1.2 Trusted Types	4
1.2.1 Threat model	4
1.2.2 Content Security Policy (CSP)	5
1.2.3 Trusted Types policies	6
1.2.4 Default policy	6
1.2.5 Reviewability	7
1.2.6 Browser support and polyfill	8
1.3 Web frameworks and libraries	9
1.3.1 Next.js	9
1.3.2 Create React App	9
1.3.3 Cypress	10
1.4 Motivation and background	10
2 Trusted Types integration	11
2.1 Locate all of the DOM sinks	11
2.1.1 Static search through the codebase	12
2.1.2 Static code analyzers	12
2.1.3 Using the target in a real world application	12
2.2 Find the most suitable workaround for every sink found	13
2.3 Implementing the integration and releasing a new version of the target	13
2.3.1 Reasoning about the integration	13
2.3.2 Trusted Types compatibility in dependencies	14
2.3.3 Knowledge required for the integration author	14
3 Trusted Types integration into Next.js	15
3.1 Fixing violations reported by Tsec	16
3.2 Fixing the dev mode of an example application	16

4	Trusted Types integration into Create React App	17
4.1	Using Trusted Types compatible version of React	17
4.2	Using Trusted Types compliant version of Webpack	17
5	Testing	21
5.1	Trusted Types plugin	21
5.1.1	Removed CSP header	21
5.1.2	Testing the violations	22
5.1.3	Releasing the plugin	24

List of Figures

List of Tables

Concepts and definitions

1. **DOM source and sink** - In the context of XSS, a DOM source is the location from which untrusted data is taken by the application (which can be controlled by user input) and passed on to the sink (e.g. location, cookies). Sinks are the places where untrusted data coming from the sources is actually getting executed resulting in DOM XSS (e.g. eval, element.innerHTML) [1]. We might also refer to sink as injection sink, because the untrusted value is injected into the sink by the attacked.
2. **Hot reload** - The concept of live or hot reloading is that the running application running in development mode is automatically restarted after code changes are made. The former restarts the whole app, the latter only patches the running application with code changed and preserves the application state.
3. **DOM XSS** - DOM Based XSS is an XSS attack wherein the attack payload is executed as a result of modifying the DOM environment in the victim's browser used by the original client side script, so that the client side code runs in an "unexpected" manner [20].
4. **CSP** - Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including XSS and data injection attacks [6]. CSP provides a way for browsers to create safer APIs in a backwards compatible manner, since the API has to be opt in explicitly by the application server by sending the CSP response header or using the CSP inside the HTML meta tag in the response body. If the browser does not support the CSP directive, the directive is ignored and standard browser behaviour applies.

Chapter 1

Introduction

1.1 Cross site scripting (XSS)

Cross site scripting (XSS) is one of the most prevalent vulnerabilities on the web. It is an attack of web applications taking untrusted user input and interpreting it as code without sanitization or escaping. The XSS has many subcategories, for this paper the most important is DOM XSS (3), where the injection happens on the client side, the browser [21].

This vulnerability became more widespread with the boom of single page applications where most of the behaviour is achieved by modifying the DOM using JavaScript. There are many functions, element attributes and properties in the DOM API which interpret the arguments as executable code. We call these DOM sinks (1). These sinks make it easy for developers to accidentally introduce this vulnerability [21].

There are many attempts to reduce the risk of DOM XSS either by dynamic or static checkers. The former usually suffer from performance and scalability issues when applied on large codebases while the latter provide suboptimal results due to JavaScript dynamic nature [21].

```
document.write()
document.writeln()
document.domain
element.innerHTML
element.insertAdjacentHTML
element.onevent
DomParser.parseFromString
frame.srdoc
eval()
script.src
Worker()
```

Listing 1.1: Examples of DOM XSS attack vectors [22] [21]

1.2 Trusted Types

Trusted Types is a relatively modern web API designed by Google based on a long history of mitigating XSS [3].

It is a browser security feature that limits access to dangerous DOM APIs to protect against DOM XSS. Trusted Types provide type guarantees to all frontend code by enforcing security type checks directly in the web browser. They are delivered through a CSP header and have a report-only mode that does not change application behavior and an enforcement mode that may cause user-observable breakages [10].

When enforced, Trusted Types block dangerous injection sinks (1) from being called with values that have not passed through a Trusted Types policy [10]. If an untrusted value is passed to sink a Trusted Types violation is raised and the DOM is unaffected. In practice this means that a potential DOM XSS has been prevented.

There are many other resources which can be used to explore Trusted Types in depth [12].

1.2.1 Threat model

Trusted Types is a powerful API with a well scoped threat model. The main goals of the API are to [14]:

- reduce the risk of client side vulnerabilities caused by injection sinks.
- replace the insecure by default APIs with safer alternatives which are hard to misuse.
- encourage a design where the code affecting the application security is encapsulated in a small part of an application.
- reduce the security review surface for applications and libraries.

The main idea behind Trusted Types is to replace the dangerous APIs with safer alternatives. It is very tempting to extend the threat model of Trusted types to cover other surfaces such as various server side attacks. However, this is a very complex area and it is part of the non goals of Trusted Types [15]. Some of the non goals include:

- preventing or mitigating server side generated markup attacks. Defending against XSS on both client and server can be really complex, especially for applications where parts of the code can run on both client and server, such as NextJS (1.3.1). To address these attacks, use the existing recommended solutions like templating systems or CSP script-src.

- controlling subresource loading. Trusted Types deal with code running in realm of the current document and does not guard subresources.
- guarding cross origin JavaScript execution, for example loading new documents via data: URLs
- protecting against malicious developers of the web application.

1.2.2 Content Security Policy (CSP)

Trusted Types are enabled through a CSP (4) using two different directives:

- *require-trusted-types-for* – This directive instructs user agents to control the data passed to DOM XSS sink functions ([16]).

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

Listing 1.2: Syntax of require-trusted-types-for directive

- *trusted-types* – This directive instructs user agents to restrict the creation of Trusted Types policies ([17]). Syntax:

```
Content-Security-Policy: trusted-types;
Content-Security-Policy: trusted-types 'none';
Content-Security-Policy: trusted-types <policyName>;
Content-Security-Policy: trusted-types <policyName> <policyName>
    'allow-duplicates';
```

Listing 1.3: Syntax of trusted-types directive

These directives together enable and configure Trusted Types behaviour for the particular web page. They allow the application authors to define rules guarding write access to the DOM sinks and thus reducing the DOM XSS attack surface to small, isolated parts of the web application codebase, facilitating their monitoring and manual code review.

Apart from the standard *Content-Security-Policy* header there is also *Content-Security-Policy-Report-Only* which can be used to enable Trusted Types in report only mode. This mode interprets Trusted Types violations only as warnings. This way the application can gradually work on Trusted Types compliance without breaking the existing application. It is also recommended to use the report only mode in production for some time to make sure the integration is working as expected [21].

Once the Trusted Types are enabled, the browser changes the behaviour of insecure DOM API sinks and expects "trusted" values instead of regular strings. These trusted values are created via Trusted Types policies.

1.2.3 Trusted Types policies

The core part of Trusted Types API are policies which are factory functions for creating "trusted" values which can be assigned to DOM sinks when Trusted Types are enabled. The policies are created by the application and access to them should be restricted. In javascript this can be easily achieved by creating a policy in its own module and exporting only a very specific functions which use this policy internally.

```
const identity = (id) => id
const createHTMLCallback = identity;
const createScriptCallback = identity;
const createScriptURLCallback = identity;
const myPolicy = window.trustedTypes.createPolicy('my-policy', {
  createHTML: createHTMLCallback,
  createScript: createScriptCallback,
  createScriptURL: createScriptURLCallback,
});
```

Listing 1.4: Creating Trusted Types policy

```
const trustedHtml = myPolicy.createHTML("<span>safe html</span>");
```

Listing 1.5: Create trusted value using a policy

The code listing 1.4 creates a Trusted Types policy using the callback functions. This callback function is called when the policy is used to create a trusted value. It receives the sink value of string type as an argument and has to return a string value that is XSS free and thus can be trusted. In practice, this function may be implemented as identity if the payload is trusted. Another good example would be to sanitize the sink value inside this callback. In case the payload should not be used, you can return *null* or *undefined* which will trigger a Trusted Types violation.

```
const myPolicy = window.trustedTypes.createPolicy('sanitize-html', {
  createHTML: (untrustedValue) => DOMPurify.sanitize(untrustedValue),
});
```

Listing 1.6: Using a policy to sanitize HTML values

1.2.4 Default policy

There is one special case for Trusted Types policies. Applications may create a policy called "default". This policy has a special behaviour. When a string value is passed to a DOM sink when Trusted Types are enforced, the user agent will implicitly flow the untrusted string value through the default policy. The callback function of the

default policy receives three arguments, the string payload, sink type and sink name respectively. This allows the application to recover from an unexpected sink usage, for example by sanitizing the untrusted value. If the default policy does not exist or returns *null* or *undefined* a CSP violation will be triggered [13]. Applications can use this policy to enable enforcement mode even though the application is not fully Trusted Types compliant.

This feature is intended to be used by applications with legacy code that uses injection sinks. The callback functions of the policy should be defined with very strict rules to prevent bypassing security restrictions enforced by Trusted Types API. For example, having an "accept all" default policy defeats the whole purpose of Trusted Types API. Developers should be very cautious when using the default policy and preferably use it only for a transition period until the legacy code is refactored not to use the dangerous DOM sinks [13].

```
trustedTypes.createPolicy('default', {
  createScriptURL: (value, type, sink) => {
    return value +
      '?default-policy-used&type=' +
      encodeURIComponent(type) +
      '&sink=' +
      encodeURIComponent(sink);
  }
});
```

Listing 1.7: Creating a default policy [13]

1.2.5 Reviewability

Consider the problem of security reviews for web applications. There are many tools and methodologies which can help reason about the application security, but there is no automated way that can assert the application safety. This means that it is still necessary for security engineers to manually review the implementation and look for potential vulnerabilities and analyze them.

When focusing on client side XSS, the engineer has to determine whether application uses dangerous DOM sinks and whether there is way for attacker to misuse them.

```
function setHtml(element, html) {
  element.innerHTML = html;
}
```

Listing 1.8: Possibly dangerous function

Is the function in the listing above safe? There is not enough information to answer this. The safety of this function depends on the context and how it is used. More generally, the safety of this function depends on both its direct and indirect callers, both present and future ones [3].

```
function processHtml(html) {  
    setHtml(document.body, html);  
}  
  
function processUserData(data) {  
    log('Processing user data');  
    // Is this safe? Can this call change "data.html"?  
    someThirdPartyCall(data);  
    processHtml(data.html);  
}
```

Listing 1.9: Usage of the possibly dangerous function

Looking for the callers of the function can be difficult because of the dynamic nature of JavaScript. Also, JavaScript is a mutable language which makes it harder to reason about function calls, especially the third party ones.

When the application enforces Trusted Types, the engineer doesn't have to care about the dangerous functions and its callers. The focus of the security review shifts to reasoning about the creation of trusted values and policies. Once a trusted value is created it is immutable and the policy which created it guarantees the security. When a trusted value reaches a sink, this guarantee still holds independently of how was the value passed around throughout the callers. Consider the third party call in the listing 1.9 and assume *data.html* contains a TrustedHTML value. If the third party call modified this value a violation would be thrown when passed to the DOM sink. It could also replace the trusted value with a different TrustedHTML value. However, the new value is again trusted, so this is not a security vulnerability, but an application bug.

1.2.6 Browser support and polyfill

Trusted Types are currently supported in Chromium family of browsers [18]. Developers creating Trusted Types compliant application should always check if Trusted Types are available in the current execution context, which does not necessary need to be a browser. It is very common for nodeJS applications to pre render the client side code on the server to provide faster experience for the end users. This brings additional complexity and new attack vectors in forms of reflected XSS, various kinds of injection and more, which are out of the threat model under which Trusted Types operate.

The nice thing is that once the application is Trusted Types compliant then all of the application sinks are protected. The application can also use a polyfill for browsers which do not support Trusted Types, which results in the same security properties as in the browsers where they are supported [9].

Browsers which do not support Trusted Types yet can use one of the variants of the polyfill:

- Full – Defines the Trusted Types API, parses the *meta* tag from the HTML and enables the enforcement in the DOM.
- API only – Defines the Trusted Types API so you can use policies and create trusted values, but no enforcement rules are applied.
- Tiny – Polyfills only the most important part of the API surface with a single line of code for minimal bundle size.

1.3 Web frameworks and libraries

Web frameworks and libraries is a software that is designed to support development of web applications and services to improve developer experience. They try to solve common problems faced in web development, such as building user interfaces, testing, building and bundling the application. Typical web application consists of numerous libraries and supporting frameworks which together create the resulting web application.

1.3.1 Next.js

Next.js is one of the most popular frameworks for building web applications. The framework is build upon React which is the most used library as of 2021 [19]. The design of Next.js allows building the application on a page by page basic to maximize the user experience. Some parts of the application can be statically rendered, some rendered server side or fully client side. Next.js is thus not only about the client side (the DOM), but it can also handle server side rendering, data processing, API requests which open up different means of attacks such as reflected XSS, SQL injections and more.

1.3.2 Create React App

Create React App is an officially supported way to create single-page React applications. It offers a modern build setup with no configuration. It is a CLI which creates

and configures a minimal React application. This is ideal for starting new projects as the configuration is abstracted away from the user.

The source code of this tool does not depend on React directly. It only generates the project files using based on hard coded template and then it installs the latest version of React and other necessary dependencies.

1.3.3 Cypress

Cypress is one of the most popular frameworks for end to end testing of web applications [7]. It enjoys a rich ecosystem of plugins and supporting software. It runs the tests in real browsers and is fast and reliable due to its unique architecture. Developers can test the Trusted Types compliant applications in Cypress out of the box, because most of the Cypress commands only query the DOM which does not produce Trusted Types violations.

1.4 Motivation and background

Trusted Types provide opportunity to significantly reduce the risk of client side XSS and has been proven in various scale projects and libraries [21] [11]. However, projects need to refactor parts of their code, which can be difficult, especially in the open source world where the software is composed by multiple dependencies which can't easily be modified. This presents a large barrier in Trusted Types adoption [21] with a "chicken and egg" problem. There is not enough pressure for library authors to migrate to Trusted Types and lot of applications are prevented to migrate because their dependencies do not work with Trusted Types.

In this paper we try to analyze some of the most popular open source frameworks and libraries and show that there are workarounds for projects to use Trusted Types without too much hassle. We also stress the need for more tooling and libraries with Trusted Types support, where we see a big opportunity for open source contributors to engage.

There is usually a knowledge gap between security engineers and software developers, the former focus on security, the latter on the application features. Trusted Types bridge this gap by providing secure by default software. The ideal scenario is if the open source libraries used Trusted Types transparently to the application authors.

Chapter 2

Trusted Types integration

Integrating Trusted Types to target applications and libraries is a might seem as complex task that requires good knowledge of the target inner workings. There is a small sample of already implemented integrations, which show that the necessary code changes are relatively small [11]. Based on our experience, the integration does not require an exptrteese of the projects inner workings. This experience is also supported by other integration authors [21]. Each integration is different, but on a high level they follow the same steps:

1. Locate all of the DOM sinks
2. Find the most suitable workaround for every sink found
3. Implement the integration and release a new version of the target

2.1 Locate all of the DOM sinks

Locating the sinks of the integration target is important for scoping the integration effort and the implementation afterwards. This task is complex since there is no bulletproof way of locating all of the sinks in a codebase. This is because JavaScript is a dynamic language and it is possible to access and set the sink values dynamically using the property element access.

Fortunately, there are a few methods and tools, which can help to catch most of the sinks:

1. Static search through the codebase
2. Static code analyzers
3. Using the target in an real world application

2.1.1 Static search through the codebase

This method is the simplest one and arguably the least effective. Statically searching for sinks throughout the codebase produces many false positives and false negatives. The former are produced for read only sink usage, the latter when actual sinks are missed due to implementation limitations. The output of the static search is usually cluttered with less important violations in tests and built tools, which you need to manually exclude from the search.

Nevertheless, this method is easy to reason about, fast to iterate and the final search results can provide a good estimate of the integration scope. This works well in practice since there is an assumption that the target source code is not malicious and doesn't actively use code patterns which are trying to hide or cause an XSS vulnerability.

There is not an actively maintained static search tool for finding DOM sinks. However, it is relatively easy to build a script, which uses the existing tools such as *grep* with a list of already known sinks [27].

2.1.2 Static code analyzers

A better approach at searching for the DOM sinks statically, is to search through the AST of the code. The quality of the output produced depends on the quality of the AST information. When the codebase is using TypeScript, the AST information is generally richer compared to codebases using JavaScript. One can then build and use tools like Tsec [31] which uses the compiler to parse the source code and create the AST to ultimately find the sinks in a more reliable manner and produces less false positives.

These tools have an advantage that they can be used to maintain the Trusted Types compatibility even after the violations are fixed. For example, they can be run in CI pipeline or their output can be leveraged by linters and other language plugin tools and the errors can be shown to the developers directly in their IDE [32].

2.1.3 Using the target in a real world application

While static search through the codebase is fast and locates most of the sinks, it usually doesn't catch them all. The author of the integration should verify the integration on the applications using the target as a dependency. Also, having good test coverage in the application code greatly increases the chance that the integration is implemented correctly.

That said, finding a suitable application might be challenging and it may not be an ideal way to test all edge cases. For example, when implementing an integration to React, one can find lot of real world applications using React, but most of them are

already XSS free so you can only verify if the integration doesn't break these clients.

One recommendation for the clients are to use the report only mode of Trusted Types CSP. This allows applications to migrate their code gradually and allows them to focus on application features.

Library authors need to test how the integration works when used with applications that uses the DOM sinks and now has to produce Trusted Types values. These are done best by creating an application from scratch by the integration author.

2.2 Find the most suitable workaround for every sink found

TODO: write me

2.3 Implementing the integration and releasing a new version of the target

Implementing the integration and releasing a new version of the target is undoubtedly an important part of Trusted Types integration. However, this can take long time for multiple reasons, which are described in separate sections:

1. Reasoning about the integration
2. Trusted Types compatibility in dependencies
3. Knowledge required for the integration author

2.3.1 Reasoning about the integration

Proving that the integration is correct means to determine if all sinks have been located and properly addressed. This is generally infeasible or impossible to determine. Project usually look at patches empirically. If the integration looks correct and is properly tested then it is safe to assume that the integration is correct. This is especially true when the integration is tested by large scale organizations by lot of services.

That being said, Trusted Types enforcement is a breaking change and project should make this change opt-in or release a new version with breaking changes [5]. If the integration is turned on by default when Trusted Types are available in the browser, the target is risking breaking existing applications [8].

Releasing an opt-in change might be problematic if the target is not configurable. This can result in the integration being put behind a feature flag which hurts the adoption [24].

2.3.2 Trusted Types compatibility in dependencies

Implementing the integration in large projects, which consists of many dependencies can bring a lot of overhead, because to be fully Trusted Types compliant one must ensure that all of the dependencies are Trusted Types compliant as well.

When there is non compliant dependency, one has multiple options:

- Implement the integration for the dependency - This option leads to recursive integrations and has all the problems already mentioned and can possibly lead to many more integrations.
- Find an alternative dependency - This option is often impossible as a viable alternative might not exist and projects might not want to use an alternative only because of Trusted Types compliance.
- Use Trusted Types default policy - This option should only be used by end applications and is more complex. The application is not fully Trusted Types compliant and it can also lead to a reduced performance.

2.3.3 Knowledge required for the integration author

The integration author can neither be a security engineer familiar with Trusted Types and neither a part of the engineering team of the target familiar with the target code. This means that the author might not be fully familiar with both of the technologies and the respective teams, which can result in both:

- Increased probability of a bug in implementation
- Harder and longer review, since the reviewers might also lack the information about Trusted Types or simply ignore the PR due to other priorities

Chapter 3

Trusted Types integration into Next.js

Next.js (described in 1.3.1) was the initial choice for Trusted Types integration, because of the large impact this integration would have. The framework itself seemed interested in the integration of Trusted Types for a longer time [30].

We forked the Next.js repository and created a basic Next.js application. We then used the local version of Next.js as a dependency for our application. The integration required a few code changes in the implementation of Next.js and we ended up with a working version which supported the application in dev mode with Trusted Types under enforcement mode. We managed to accomplish this with one simply Trusted Types policy in a couple of days.

```
let policy

const whitelistAll = (str) => str;

// The policy getter is a private part of the module
// and cannot be used directly.
const getOrCreatePolicy = () => {
  if (policy) return policy

  policy = window.trustedTypes?.createPolicy('next', {
    createHTML: whitelistAll('createHTML'),
    createScript: whitelistAll('createScript'),
    createScriptURL: whitelistAll('createScriptURL'),
  })
  return policy
}

export const __unsafeAllowHtml = (html) => getOrCreatePolicy()?.
  createHTML(html) ?? html

export const __unsafeAllowScriptUrl = (scriptUrl) => getOrCreatePolicy
  ()?.createScriptURL(scriptUrl) ?? scriptUrl
```

```
export const __unsafeAllowScript = (script) => getOrCreatePolicy()?.  
  createScript(script) ?? script
```

Listing 3.1: Example of Next.js Trusted Types API

The fixes needed were small the Trusted Types API specific for Next.js was encapsulated in a single small module. That said, the implementation was only a proof of concept and the policy implemented might have allowed more than necessary. However, we decided not to pursue this project no more due to different priorities and shifted focus to a different project.

3.1 Fixing violations reported by Tsec

Tsec found 8 violations [29] inside Next.js sources. Out of these 7 were indeed Trusted Types violations that needed to be fixed. Some of these could be fixed simply on a type system level since they expected a value from the user. The others needed to be allowed explicitly by using a policy. The implementation for this proof of concept can be found on github [28].

Since our utmost goal was to find the sinks and create a prototype for the integration we wrapped all of these values in Trusted Types objects. This was to be revisited in the future.

3.2 Fixing the dev mode of an example application

Fixing the violations found by Tsec was not enough and the application still wouldn't launch with Trusted Types enforced. The reason for this hasn't been clear, but it was probably a webpack plugin used in one of the Next.js dependencies. The violating code relied on `eval`, which threw an error when Trusted Types were enforced. The workaround for this was to use a default policy and allow all `eval` calls.

Apart from this, there was another violation that was triggered caused by application hot reloading (2). Tsec wasn't able to catch this, since the violation came from a JavaScript file where the AST information was limited.

Chapter 4

Trusted Types integration into Create React App

Create React App (CRA) (described in 1.3.2) was a second project we wanted to integrate Trusted Types to. After taking a look in the implementation of CRA we found that this tool does not depend on React directly, but only installs it after creating the project template. Our goal shifted to make sure the generated project by CRA is Trusted Types compatible.

4.1 Using Trusted Types compatible version of React

To accomplish this, we would need to change the implementation of CRA to install Trusted Types compatible version of React. Unfortunately, such version of React is implemented under a feature flag which needs to be turned on at build time. The published version of React contains the already built files with the feature flag turned off. This means that if you want to use the Trusted Types compatible version of React you have to clone the React repository from sources, turn on the feature flag and then build the framework. You can then use this version of React as a dependency in your project generated by CRA.

Implementing this is non trivial, since it requires knowledge about React. More importantly though, this is harder to maintain for the application authors since you need to keep up with the new releases of React manually.

4.2 Using Trusted Types compliant version of Webpack

CRA internally uses webpack version 5 to provide fast development experience with convenient features, such as hot reload. It also bundles the application for production

and it handles minification and other optimizations. Some of these features, especially hot reload breaks under Trusted Types in enforcement mode. Gladly, webpack can be configured to be Trusted Types compliant by a small configuration change [23].

The problem with CRA is that the webpack configuration is abstracted away from the user. This means that there is not a simple way how to enable the Trusted Types integration. One can find the webpack configuration in the downloaded dependencies and change it there directly, but this won't really work since those changes will be removed by the package manager when modifying the dependencies. In general, one should never modify the contents of dependencies and treat it only as read only inputs to the program.

The optimal solution as of now is to use a workaround which allows you to spy on modules and change what they return. This pattern is often used when mocking or spying in unit tests. However, it is also a suitable solution for this case [2]. CRA team is reluctant to change this, since the hidden configuration is a good default for the majority of users.

```
// File 'scripts/start.js'
const rewire = require('rewire')
const defaults = rewire('react-scripts/scripts/start.js')
const webpackConfig = require('react-scripts/config/webpack.config')

// In order to override the webpack configuration without ejecting the
// create-react-app
defaults.__set__('configFactory', (webpackEnv) => {
  let config = webpackConfig(webpackEnv)

  // Customize the webpack configuration here, for reference I have
  // updated webpack externals field
  config.output.trustedTypes = {
    policyName: 'webpack-policy',
  }

  return config
})
```

Listing 4.1: Script to start React application with Trusted Types enabled in webpack

The application is then started simply by running this script using node.

```
node ./scripts/start
```

Listing 4.2: Running the application

Another option is to use the *eject* command from CRA. This is a one way operation and it essentially unwraps all of the hidden configuration and creates these files in your

project. You can then simply edit the webpack configuration which is now part of your project. This is not recommended and it should be used only when all other attempts fail. The generated webpack configuration is pretty complex and updating it in the future might not be trivial.

Chapter 5

Testing

Trusted Types are agnostic to the testing framework used and the type of tests. It is very common for web application to have a combination of unit and end to end tests. The former are used to smaller parts of application and typically run in nodeJS environment. The latter usually test the whole application in browser environment and test the application features from the user perspective.

5.1 Trusted Types plugin

Even though Cypress (1.3.3) supports Trusted Types out of the box, there are a few nuances the developer has to overcome to be able to test the application and Trusted Types violations. For this reason, we have created a Cypress plugin which abstracts the low level details and provides a nicer API for the developers to use.

5.1.1 Removed CSP header

Cypress removes the CSP header sent by the application server in order to load the application in an iframe, which could otherwise be prevented by a *scriptSrc* CSP directive. There is a workaround for now, which is to intercept the request of the initial HTML application payload and copy the CSP policy from the response headers to the response body inside a *meta* tag. [4].

This is tedious for the developers, so we have created a custom command in our plugin which does exactly this.

```
// NOTE: Based on https://glebbahmutov.com/blog/testing-csp-almost/
Cypress.Commands.add('enableCspThroughMetaTag', (options) => {
  const { urlPattern } = options ?? {};

  // Intercept all requests by default
  cy.intercept(urlPattern ?? '**/*', (req) => {
```

```

return req.reply((res) => {
  const csp = res.headers['content-security-policy'];
  if (!csp || typeof res.body !== 'string') return;

  res.body = res.body
    .replace(
      new RegExp('<head>([\\s\\S]*)</head>'),
      new RegExp('<head><meta http-equiv="Content-Security-Policy"
content="$${csp}">$1</head>').toString()
    )
    // The following are needed because the regex replacement
    // above inserts some characters
    .replace('/<head>', '<head>')
    .replace('<\\/>', '</>');
});
}).as('enableCspThroughMetaTag');
});

```

Listing 5.1: Intercept requests and enable CSP header inside via meta tag

5.1.2 Testing the violations

While it is easy to test that the Trusted Types are supported (5.2) it is harder to test whether some part of the code triggered Trusted Types violation. The reason is that the violation does not produce any user visible behaviour because the DOM is unchanged and uncaught exception is thrown and Cypress automatically fails the test. The developer needs to listen to *uncaught:exception* handler from Cypress and explicitly recognize the Trusted Types violation based on the error thrown and tell Cypress that this error is intended so it doesn't fail the test.

```

it('supports TT', () => {
  expect(window.trustedTypes).not.to.be.undefined;
});

```

Listing 5.2: Test Trusted Types support

To simplify this low level handling for the developers we have created a custom command which recognizes Trusted Types violations and remembers them for the lifetime of the current test so they can be asserted later on.

```

Cypress.Commands.add('catchTrustedTypesViolations', () => {
  if (catchTrustedTypesViolationsEnabled) return;
  catchTrustedTypesViolationsEnabled = true;
  cy.clearTrustedTypesViolations();
});

```

```

// https://docs.cypress.io/api/events/catalog-of-events#To-catch-a-
// single-uncaught-exception
cy.on('uncaught:exception', (err) => {
  const type = violationTypes.find((type) => err.message.includes(
    quote(type)));
  if (type) {
    trustedTypesViolations.push({
      type,
      message: extractViolationMessage(err),
      error: err,
    });
    // Return false to prevent the error from failing this test
    return false;
  }
});
});

```

Listing 5.3: Custom command to catch Trusted Types violations

The final part of the plugin is the API to assert the caught violations. There are multiple commands which assert that certain types of violations happened. An example of a full Cypress test which asserts the violation is listed in (5.4).

```

it('assertTrustedTypesViolations', () => {
  cy.contains('unsafe html').click();
  cy.contains('unsafe html').click();
  cy.contains('duplicate policy').click();
  cy.contains('unsafe script').click();

  cy.assertTrustedTypesViolations([
    {
      type: 'TrustedHTML',
      message:
        "Failed to set the 'srcdoc' property on 'HTMLIFrameElement': " +
        "This document requires 'TrustedHTML' assignment.",
    },
    {}, // No assertion is made for this violation
    {
      type: 'TrustedTypePolicyFactory',
      message: 'Failed to execute 'createPolicy' on ' ' +
        'TrustedTypePolicyFactory': Policy with name "my-policy" already ' +
        'exists.',
    },
    { type: 'TrustedScript' },
  ]);
});

```

Listing 5.4: Example Trusted Types violation test

5.1.3 Releasing the plugin

The plugin is implemented in a standalone repository [25] and published as an npm package [26] for everyone to use. Together with the plugin API there is an example application and tests which showcase the plugin in action. The plugin is also pending to be added to the cypress community list of plugins for increased visibility.

Bibliography

- [1] Anirudh Anand. Xss dom source and sink definition, February 2019. <https://blog.0daylabs.com/2019/02/24/learning-DomXSS-with-DomGoat/#source>.
- [2] ashvin777. Modify webpack configuration in cra (issue comment). <https://github.com/facebook/create-react-app/issues/10307#issuecomment-898889701>.
- [3] Multiple authors. Trusted types design history, September 2019. <https://github.com/w3c/webappsec-trusted-types/wiki/design-history/8a57f5cb1a7773cfa512943e9b7560813d61a83f#why-client-side-trusted-types>.
- [4] Gleb Bahmutov. Figure out how to load site with content-security-policy without stripping header (github issue). <https://github.com/cypress-io/cypress/issues/1030#>.
- [5] cure53. Dompurify 2.0.0 release. <https://github.com/cure53/DOMPurify/releases/tag/2.0.0>.
- [6] MDN Web Docs. Content security policy (csp). <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>.
- [7] Sacha Greif and team. State of js 2021 - testing. <https://2021.stateofjs.com/en-US/libraries/testing>.
- [8] Uzlopak (DOMPurify issue #361). Trusted types breaking applications using dompurify in chrome 77. <https://github.com/cure53/DOMPurify/issues/361>.
- [9] Krzysztof Kotowicz. Trusted types increase security also in browsers without tt support. <https://github.com/w3c/webappsec-trusted-types/wiki/FAQ#do-trusted-types-address-dom-xss-only-in-browsers-supporting-trusted-types>.
- [10] Krzysztof Kotowicz. Trusted types background, December 2021. <https://github.com/w3c/webappsec-trusted-types/wiki/>

- Effects-of-deploying-Trusted-Types-on-browser-extension-developers/
c110df6329c46363c65e3c3de4ef24c5fbcecee9#background.
- [11] Krzysztof Kotowicz. Trusted types integrations, November 2021. <https://github.com/w3c/webappsec-trusted-types/wiki/Integrations/3e5ff5b7613f18c15a1895129fec063d5491ff83>.
- [12] Krzysztof Kotowicz. Trusted types resources, July 2021. <https://github.com/w3c/webappsec-trusted-types/wiki/Resources/22dcd3a4cc55fae2e1706b47f9d26feb2aacaefb>.
- [13] Krzysztof Kotowicz (Google LLC) and Mike West (Google LLC). Default policy. <https://w3c.github.io/webappsec-trusted-types/dist/spec/#default-policy-hdr>.
- [14] Krzysztof Kotowicz (Google LLC) and Mike West (Google LLC). Trusted types goals. <https://w3c.github.io/webappsec-trusted-types/dist/spec/#goals>.
- [15] Krzysztof Kotowicz (Google LLC) and Mike West (Google LLC). Trusted types goals. <https://w3c.github.io/webappsec-trusted-types/dist/spec/#non-goals>.
- [16] MDN. Csp: require-trusted-types-for. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/require-trusted-types-for>.
- [17] MDN. Csp: trusted-types. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/trusted-types>.
- [18] MDN. Trusted types compatibility. https://developer.mozilla.org/en-US/docs/Web/API/Trusted_Types_API#browser_compatibility.
- [19] Stack overflow insights. Web frameworks statistics for 2021, 2021. <https://insights.stackoverflow.com/survey/2021#section-most-popular-technologies-web-frameworks>.
- [20] OWASP. Dom based xss. https://owasp.org/www-community/attacks/DOM_Based_XSS.
- [21] Krzysztof Kotowicz Pei Wang, Bjarki Ágúst Guðmundsson. Adopting trusted types in production web frameworks to prevent dom-based cross-site scripting: A case study. <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/9c56e856f0ea76454f01cabec9959f7c5b31b285.pdf>.

- [22] Portswigger. Dom-based xss. <https://portswigger.net/web-security/cross-site-scripting/dom-based>.
- [23] Webpack team. Webpack trusted types documentation. <https://webpack.js.org/configuration/output/#outputtrustedtypes>.
- [24] Emanuel Tesar. Add trusted types to react on client side pr. <https://github.com/facebook/react/pull/16157>.
- [25] Emanuel Tesar. cypress-trusted-types (github). <https://github.com/Siegrift/cypress-trusted-types>.
- [26] Emanuel Tesar. cypress-trusted-types (npm). <https://www.npmjs.com/package/@siegrift/cypress-trusted-types>.
- [27] Emanuel Tesar. Static xss code scanner. <https://github.com/Siegrift/xss-sink-finder/tree/5c98c3e80e16c15bda2ccc0609288cc536601a83>.
- [28] Emanuel Tesar. Fix tsec violations in next.js, October 2021. <https://github.com/Siegrift/next.js/commit/a45df82d5e86f7cbaa9f0e327f1b4ea0e956fbdf>.
- [29] Emanuel Tesar. Tsec output for next.js, October 2021. <https://github.com/Siegrift/next.js/blob/a45df82d5e86f7cbaa9f0e327f1b4ea0e956fbdf/tsec-packages-next-output>.
- [30] TyMick. Add trusted types policy (next.js pr), 2020. <https://github.com/vercel/next.js/pull/13509>.
- [31] Google (unofficial product). Tsec. <https://github.com/google/tsec/commit/a57933da74af5aef5fd2342f207b03c4fe305003>.
- [32] Google (unofficial product). Tsec language service plugin documentation. <https://github.com/google/tsec/tree/a57933da74af5aef5fd2342f207b03c4fe305003#language-service-plugin>.