cure53 / **DOMPurify** Public

Code Issues 1 Pull requests 2 Actions Projects Wiki Securi

Commit `302b51d`

cure53 committed on Mar 3 · 5 / 5 · Verified

```
fix: Expanded the regex ever so slightly to also cover script
```

`main` (#1205) · 3.3.3

1 parent `cd85175` commit `302b51d`

10 files changed +13 -11 lines changed

Top

Filter files…

- dist
  - purify.cjs.js.map
  - purify.cjs.js
  - purify.es.mjs.map
  - purify.es.mjs
  - purify.js.map
  - purify.js
  - purify.min.js.map
  - purify.min.js
- src
  - purify.ts
- test/fixtures
  - expect.mjs

10 files changed +13 -11 lines changed

Search within code

dist/purify.cjs.js

Load Diff

Some generated files are not rendered by default. Learn more about customizing how changed files appear on GitHub.

dist/purify.cjs.js.map

Load Diff

Some generated files are not rendered by default. Learn more about customizing how changed files appear on GitHub.

dist/purify.es.mjs

```
@@ -1121,7 +1121,7 @@ function createDOMPurify() {
1121 1121           value = SANITIZE_NAMED_PROPS_PREFIX + value;
1122 1122         }
1123 1123         /* Work around a security issue with comments inside attributes */
1124      -       if (SAFE_FOR_XML && regExpTest(/((--!?|])>)|<\/(style|title|xmp|textarea|noscript|iframe|noembed|noframes)/i, value)) {
     1124 +       if (SAFE_FOR_XML && regExpTest(/((--!?|])>)|<\/(style|script|title|xmp|textarea|noscript|iframe|noembed|noframes)/i, value)) {
1125 1125           _removeAttribute(name, currentNode);
1126 1126           continue;
1127 1127         }
```

dist/purify.es.mjs.map

Load Diff

Some generated files are not rendered by default. Learn more about customizing how changed files appear on GitHub.

dist/purify.js

Load Diff

Some generated files are not rendered by default. Learn more about customizing how changed files appear on GitHub.

dist/purify.js.map

Load Diff

Some generated files are not rendered by default. Learn more about customizing how changed files appear on GitHub.

dist/purify.min.js

Load Diff

Some generated files are not rendered by default. Learn more about customizing how changed files appear on GitHub.

dist/purify.min.js.map

Load Diff

Some generated files are not rendered by default. Learn more about customizing how changed files appear on GitHub.

src/purify.ts

```
@@ -1383,7 +1383,7 @@ function createDOMPurify(window: WindowLike =
getGlobal()): DOMPurify {
1383  1383          if (
1384  1384            SAFE_FOR_XML &&
1385  1385            regExpTest(
```

```
1386      -           /((--!?|])>)|
            <\/(style|title|xmp|textarea|noscript|iframe|noembed|noframes)/i,
      1386  +           /((--!?|])>)|
            <\/(style|script|title|xmp|textarea|noscript|iframe|noembed|noframes)/i,
1387  1387              value
1388  1388            )
1389  1389          ) {
```

test/fixtures/expect.mjs

```
      @@ -556,7 +556,8 @@ export default [
556   556              "<div id=\"102\"><img src=\"x`
           `&lt;script&gt;alert(102)&lt;/script&gt;\">//[\"'`--&gt;]]&gt;]</div>",
557   557              "<div id=\"102\"><img src=\"x` `<script>alert(102)
           </script>\">//[\"'`--&gt;]]&gt;]</div>",
558   558              "<div id=\"102\"><img
           src=\"x%60%20%60%3Cscript%3Ealert%28102%29%3C/script%3E\">//[\"'`--&gt;]]&gt;]
           </div>",
559       -            "<div id=\"102\">//[\"'`--&gt;]]&gt;]</div>"
          559  +            "<div id=\"102\">//[\"'`--&gt;]]&gt;]</div>",
          560  +            "<div id=\"102\"><img>//[\"'`--&gt;]]&gt;]</div>"
560   561          ]
561   562        }, {
562   563          "payload": "<div id=\"103\">
           <script>history.pushState(0,0,'/i/am/somewhere_else');</script>//[\"'`-->]]>]
           </div><div id=\"104\"><svg xmlns=\"http://www.w3.org/2000/svg\" id=\"foo\">\n<x
           xmlns=\"http://www.w3.org/2001/xml-events\" event=\"load\" observer=\"foo\"
           handler=\"data:image/svg+xml,%3Csvg%20xmlns%3D%22http%3A%2F%2Fwww.w3.org%2F2000
           %2Fsvg%22%3E%0A%3Chandler%20xml%3Aid%3D%22bar%22%20type%3D%22application%2Fecma
           script%22%3E alert(104)
           %3C%2Fhandler%3E%0A%3C%2Fsvg%3E%0A#bar\"/>\n</svg>//[\"'`-->]]>]</div>",
      @@ -698,7 +699,8 @@ export default [
698   699          "payload": "<div id=\"129\"><svg><image
           style='filter:url(\"data:image/svg+xml,<svg
           xmlns=%22http://www.w3.org/2000/svg%22><script>parent.alert(129)</script>
           </svg>\")'>\n<!--\nSame effect with\n<image filter='...'>\n-->\n</svg>//[\"'`--
           >]]>]</div>",
699   700          "expected": [
```

```
700  701            "<div id=\"129\"><svg><image
                    style=\"filter:url(&quot;data:image/svg+xml,&lt;svg
                    xmlns=%22http://www.w3.org/2000/svg%22&gt;&lt;script&gt;parent.alert(129)&lt;/s
                    cript&gt;&lt;/svg&gt;&quot;)\">\n\n</image></svg>//[\"'`--&gt;]]&gt;]</div>",
701      -     "<div id=\"129\"><svg><image
                    style=\"filter:url(&quot;data:image/svg+xml,<svg
                    xmlns=%22http://www.w3.org/2000/svg%22><script>parent.alert(129)</script>
                    </svg>&quot;)\">\n\n</image></svg>//[\"'`--&gt;]]&gt;]</div>"
         702 +     "<div id=\"129\"><svg><image
                    style=\"filter:url(&quot;data:image/svg+xml,<svg
                    xmlns=%22http://www.w3.org/2000/svg%22><script>parent.alert(129)</script>
                    </svg>&quot;)\">\n\n</image></svg>//[\"'`--&gt;]]&gt;]</div>",
         703 +     "<div id=\"129\"><svg><image>\n\n</image></svg>//[\"'`--&gt;]]&gt;]
                    </div>"
702  704          ]
703  705        }, {
704  706          "title": "MathML",
```

Comments 0

Please sign in to comment.