Brandenburgische
Technische Universität
Cottbus

16.07.2022

Automatische statische Analyse

Leaflet JS

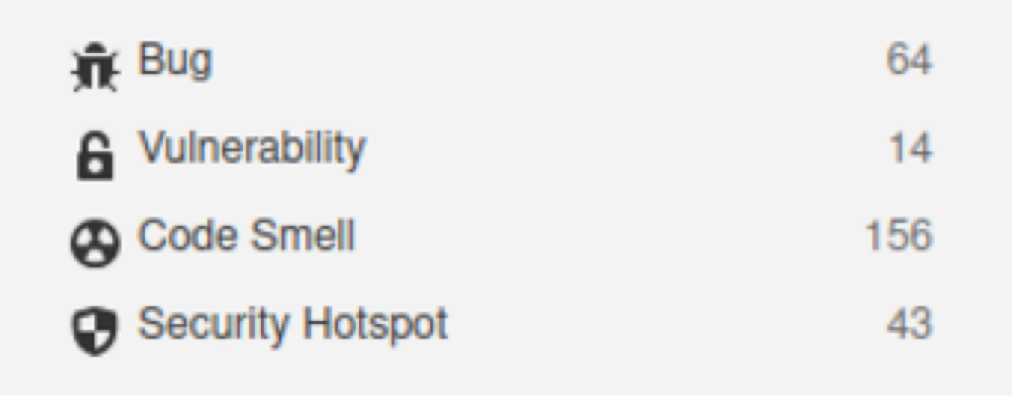
Ahmad Albenny

Brandenburgische Technische Universität Cottbus

- Unter welchen Umständen wurde die Analyse durchgeführt ?
  - Ubuntu 20.0
  - Sonarqube Version 9.5.0.56709
  - SonarQube Scanner 4.2.0.1873
  - PostgreSQL 12.1
  - Node.js 12

https://github.com/Leaflet/Leaflet Branche : main am 11.07.2022

- Metrics in ASA
  - Es wurde 277 Metrics benutzt, um den Code zu (charakterisieren) testen.
  - Bestehen aus:



- Bug Metrics (64)
  - um nur einige zu nennen:
    - "delete" should be used only with object properties
    - "NaN" should not be used in comparisons
    - "new" operators should be used with functions
    - "super()" should be invoked appropriately
    - "Symbol" should not be used as a constructor
    - Function argument names should be unique
    - A "for" loop update clause should move the counter in the right direction
    - All code should be reachable

Automatische statische Analyse
Bug Metrics (64)

Brandenburgische Technische Universität Cottbus

Function argument names should be unique

javascript:S1536

Bug Major No tags Available Since Jul 11, 2022 SonarQube (JavaScript) Constant/issue: 5min

Function arguments should all have different names to prevent any ambiguity. Indeed, if arguments have the same name, the last duplicated argument hides all the previous arguments with the same name (those previous arguments remain available through arguments[i], so they're not completely inaccessible).

This hiding makes no sense, reduces understandability and maintainability, and obviously can be error prone. Furthermore, in strict mode, declaring arguments with the same name produces an error.

Noncompliant Code Example

```
function compute(a, a, c) { // Noncompliant
}
```

Compliant Solution

```
function compute(a, b, c) { // Compliant
}
```

Extend Description

Quality Profiles

Sonar way BUILT-IN Major

- Schwachstelle Metrics (14)
  - um nur einige zu nennen:
    - File uploads should be restricted
    - JWT should be signed and verified with strong cipher algorithms
    - Origins should be verified during cross-origin communications
    - Server certificates should be verified during SSL/TLS connections
    - Server hostnames should be verified during SSL/TLS connections
    - Weak SSL/TLS protocols should not be used
    - XML parsers should not be vulnerable to XXE attacks

Automatische statische Analyse
Schwachstelle Metrics (14)

Brandenburgische Technische Universität Cottbus

A new session should be created during user authentication

javascript:S5876

Vulnerability | Critical | cwe, owasp-a2 | Available Since Jul 11, 2022 | SonarQube (JavaScript) | Constant/issue: 5min

Session fixation attacks occur when an attacker can force a legitimate user to use a session ID that he knows. To avoid fixation attacks, it's a good practice to generate a new session each time a user authenticates and delete/invalidate the existing session (the one possibly known by the attacker).

Noncompliant Code Example

For Passport.js:

```
app.post('/login',
  passport.authenticate('local', { failureRedirect: '/login' }),
  function(req, res) {
    // Sensitive - no session.regenerate after login
    res.redirect('/');
  });
```

Compliant Solution

For Passport.js:

```
app.post('/login',
  passport.authenticate('local', { failureRedirect: '/login' }),
  function(req, res) {
    let prevSession = req.session;
    req.session.regenerate((err) => {  // Compliant
      Object.assign(req.session, prevSession);
      res.redirect('/');
    });
  });
```

- Code smells Metrics (156)
  - um nur einige zu nennen:
    - Lines should not be too long
    - "continue" should not be used
    - "default" clauses should be last
    - "delete" should not be used on arrays
    - "for in" should not be used with iterables
    - "future reserved words" should not be used as identifiers
    - "if ... else if" constructs should end with "else" clauses

Automatische statische Analyse
Code smells Metrics (156)

Brandenburgische Technische Universität Cottbus

Lines should not be too long

Code Smell | Major | convention | Available Since Jul 11, 2022 | SonarQube (JavaScript) | Constant/issue: 1min

Having to scroll horizontally makes it harder to get a quick overview and understanding of any piece of code.

Extend Description

Parameters

maximumLineLength The maximum authorized line length.

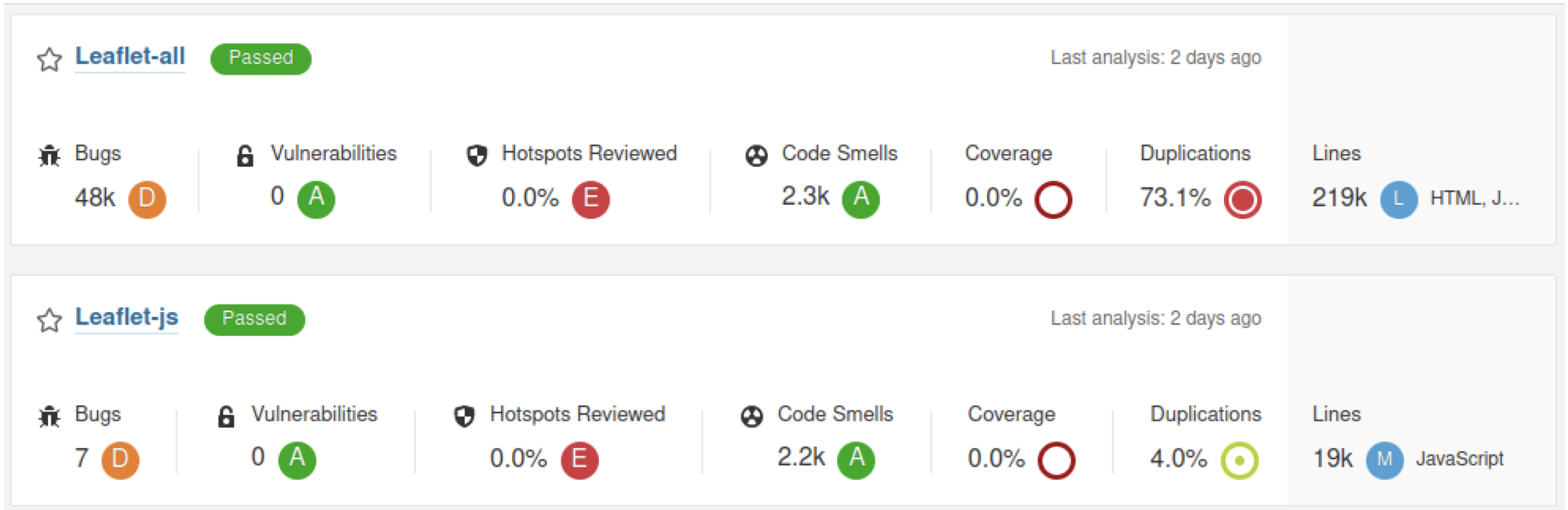
Default Value:
180

Quality Profiles

- Sicherheits-Hotspot Metrics (43)
  - um nur einige zu nennen:
    - Allowing browsers to perform DNS prefetching is security-sensitive
    - Allowing browsers to sniff MIME types is security-sensitive
    - Allowing confidential information to be logged is security-sensitive
    - Allowing mixed-content is security-sensitive
    - Allowing requests with excessive content length is security-sensitive
    - Creating cookies without the "HttpOnly" flag is security-sensitive
    - Creating cookies without the "secure" flag is security-sensitive

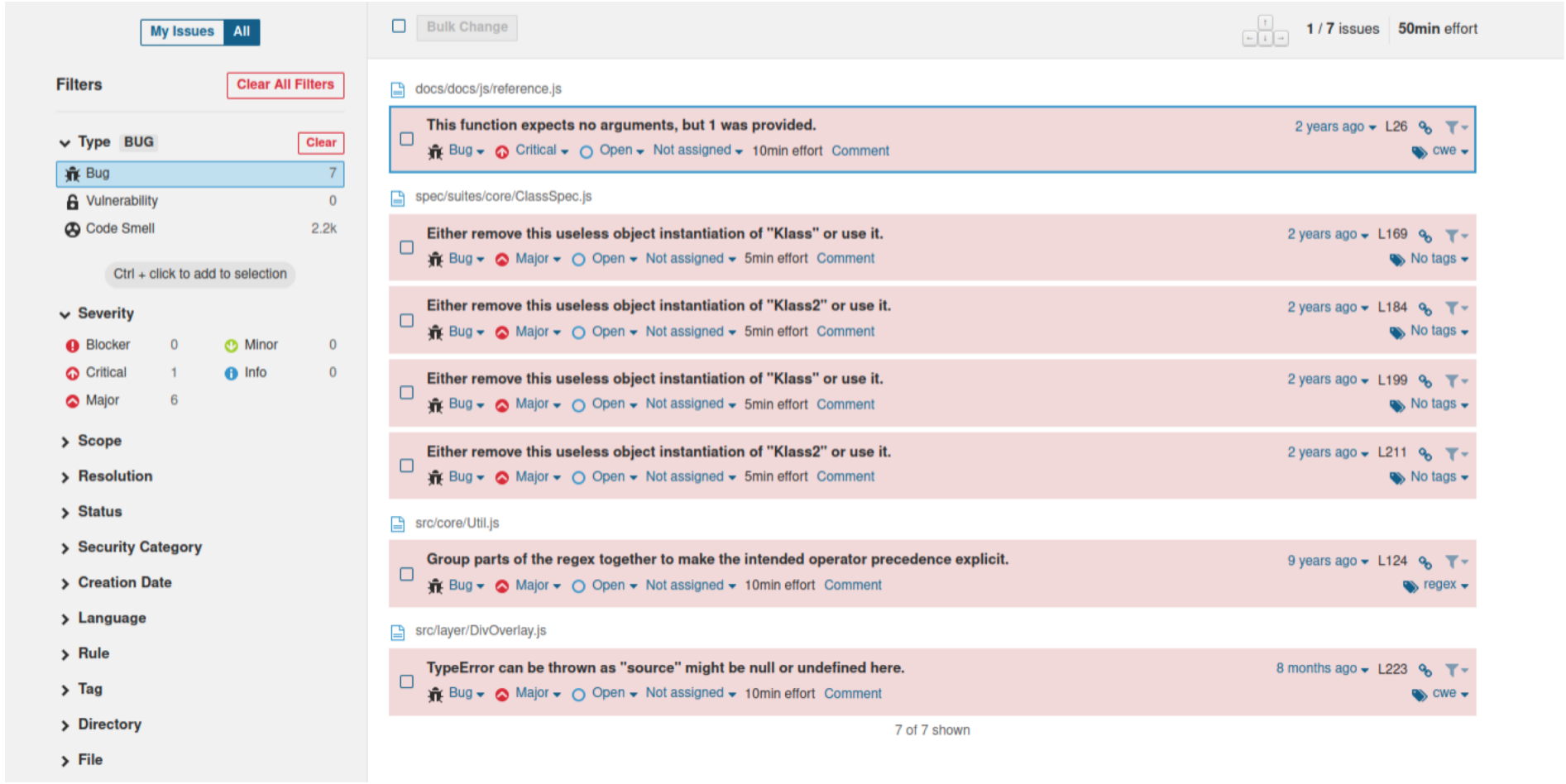
Automatische statische Analyse
Übersicht

Brandenburgische Technische Universität Cottbus



Automatische statische Analyse
Bug

Brandenburgische Technische Universität Cottbus



Automatische statische Analyse
Bug

Brandenburgische Technische Universität Cottbus

Where is the issue? | Why is this an issue?

```
15  simon…          // For table rows, insert the anchor inside the first <td>
16                  el.querySelector('td').appendChild(anchor);
17
18                  // Clicking on the row (meaning "the link icon on the ::before)
19                  // jumps to the item
20                  el.parentNode.onclick = 1 function () {
21                      return function (ev) {
22                          if (ev.offsetX < 0) {
23                              window.location.hash = '#' + ev.target.parentNode.id;
24                          }
25                      };
26                  }( 2 el.id);
```

This function expects no arguments, but 1 was provided. 2 years ago L26

Bug Critical Open Not assigned 10min effort Comment cwe

```
27              }
28          }
29      }
30
31      elems = document.querySelectorAll('div.accordion');
32      for (i = 0, len = elems.length; i < len; i++) {
33          el = elems[i];
34
35          el.querySelector('label').addEventListener('click', function (c) {
```

Automatische statische Analyse
Bug

Brandenburgische Technische Universität Cottbus

Either remove this useless object instantiation of "Klass2" or use it.

Objects should not be created to be dropped immediately without being used javascript:S1848

Where is the issue? | Why is this an issue?

Leaflet-js spec/suites/core/ClassSpec.js See all issues in this file

```
179 jacob…          var Klass2 = Klass.extend({});
180
181 agafo…          Klass.addInitHook(spy1);
182 jacob…          Klass2.addInitHook(spy2);
183
184 johnd…          new Klass2();
```

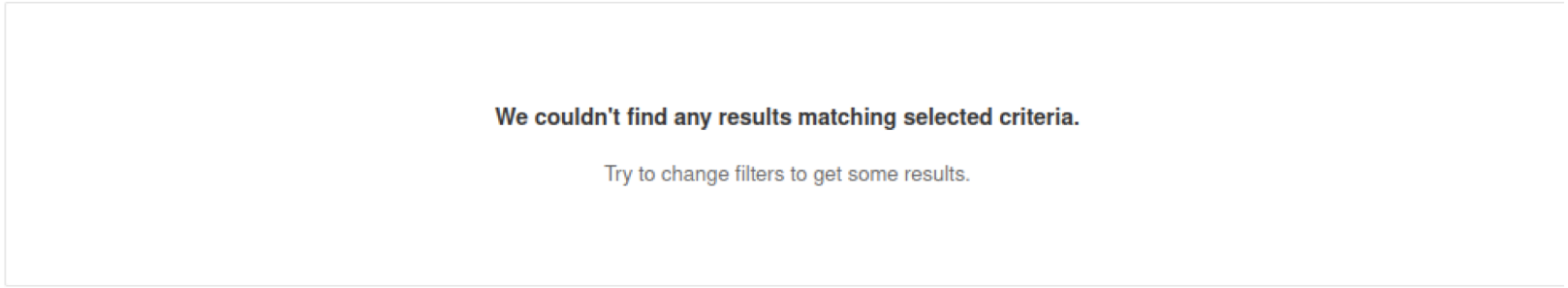
Either remove this useless object instantiation of "Klass2" or use it. 2 years ago L184

Bug Major Open Not assigned 5min effort Comment No tags

```
185 jacob…
186 tom@m…          expect(spy1.called).to.be.ok();
187                  expect(spy2.called).to.be.ok();
188 jacob…      });
189
190 john.…      it("does not call child constructor hooks", function () {
191 tom@m…          var spy1 = sinon.spy(),
192                      spy2 = sinon.spy();
193 agafo…
```

Automatische statische Analyse
Schwachstelle

Brandenburgische
Technische Universität
Cottbus



Automatische statische Analyse
Code smells (2.2k)

Brandenburgische Technische Universität Cottbus

build/integrity.js

Unexpected var, use let or const instead. — 5 years ago · L4
Code Smell · Critical · Open · Not assigned · 5min effort · Comment — bad-practice, es2015

Unexpected var, use let or const instead. — 5 years ago · L5
Code Smell · Critical · Open · Not assigned · 5min effort · Comment — bad-practice, es2015

Unexpected var, use let or const instead. — 5 years ago · L6
Code Smell · Critical · Open · Not assigned · 5min effort · Comment — bad-practice, es2015

Unexpected var, use let or const instead. — 5 years ago · L18
Code Smell · Critical · Open · Not assigned · 5min effort · Comment — bad-practice, es2015

Remove this commented out code. — 5 years ago · L26
Code Smell · Major · Open · Not assigned · 5min effort · Comment — unused

build/rollup-config.js

Rename this file to "config" — 4 months ago
Code Smell · Minor · Open · Not assigned · 5min effort · Comment — confusing, convention, es2015

debug/vector/geojson-sample.js

Unexpected var, use let or const instead. — 10 years ago · L53
Code Smell · Critical · Open · Not assigned · 5min effort · Comment — bad-practice, es2015

Automatische statische Analyse
Code smells (2.2k)

Brandenburgische Technische Universität Cottbus

Unexpected var, use let or const instead.

Variables should be declared with "let" or "const" javascript:S3504

Where is the issue? | Why is this an issue?

Leaflet-js | build/docs.js | See all issues in this file

```
1  simon…  console.log('Building Leaflet documentation with Leafdoc ...');
2  ivan@…
3          var LeafDoc = require('leafdoc');
```

Unexpected var, use let or const instead. 6 years ago · L3

Code Smell · Critical · Open · Not assigned · 5min effort · Comment · bad-practice, es2015

```
4          var doc = new LeafDoc({
5              templateDir: 'build/leafdoc-templates',
6  yb@en…      showInheritancesWhenEmpty: true,
7              leadingCharacter: '@'
8  ivan@…  });
```

Unexpected var, use let or const instead.

```
9
10         // Note to Vladimir: Iván's never gonna uncomment the following line. He's
11         // too proud of the little leaves around the code.
12         // doc.setLeadingChar('@');
```

Automatische statische Analyse
Code smells (2.2k)

Brandenburgische Technische Universität Cottbus

Consider moving declaration of 'i' as it is referenced outside current binding context.

Variables should be used in the blocks where they are declared javascript:S2392

Where is the issue? | Why is this an issue?

Leaflet-js docs/docs/js/reference.js See all issues in this file

```
1  simon…  if (document.body.className.indexOf('api-page') !== -1) {
2
3              var elems = document.querySelectorAll('h2, h3, h4, tr');
               Unexpected var, use let or const instead.
4
5              for (var i = 0, len = elems.length; i < len; i++) {
               Unexpected var, use let or const instead.
               Consider moving declaration of 'i' as it is referenced outside current binding context.
               2 years ago L5
               Code Smell Major Open Not assigned 2min effort Comment
               pitfall
               Consider moving declaration of 'len' as it is referenced outside current binding context.
6                  var el = elems[i];
               Unexpected var, use let or const instead.
               Consider moving declaration of 'el' as it is referenced outside current binding context.
7
8                  if (el.id) {
```

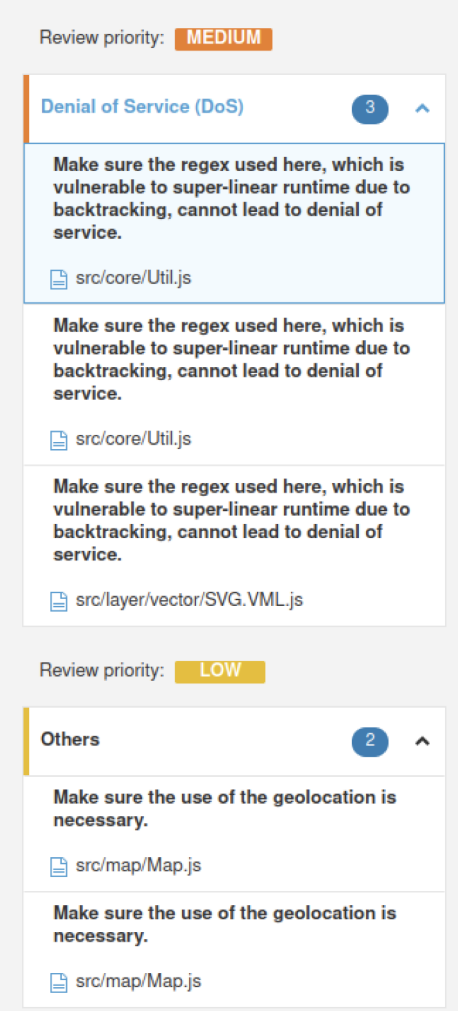
Automatische statische Analyse
Code smells (2.2k)

Brandenburgische Technische Universität Cottbus

```
27  simon…              }
28                  }
29              }
30
31              elems = document.querySelectorAll('div.accordion');
32              for ( 1 i = 0, len = elems.length;  2 i < len;  3 i++) {
33                  el = elems[ 4 i];
34
35                  el.querySelector('label').addEventListener('click', function (c) {
36                      return function () {
37                          if (c.className === 'accordion expanded') {
38                              c.className = 'accordion collapsed';
```

Automatische statische Analyse
Sicherheits-Hotspot (5)

Brandenburgische Technische Universität Cottbus



Automatische statische Analyse
Sicherheits-Hotspot (5)

Brandenburgische Technische Universität Cottbus

Make sure the regex used here, which is vulnerable to super-linear runtime due to backtracking, cannot lead to denial of service.

Using slow regular expressions is security-sensitive javascript:S5852

Status: TO REVIEW

This security hotspot needs to be reviewed to assess whether the code poses a risk.

Change status

Assignee: **Not assigned**

Where is the risk? | What's the risk? | Assess the risk | How can you fix it?

src/core/Util.js

Open in IDE

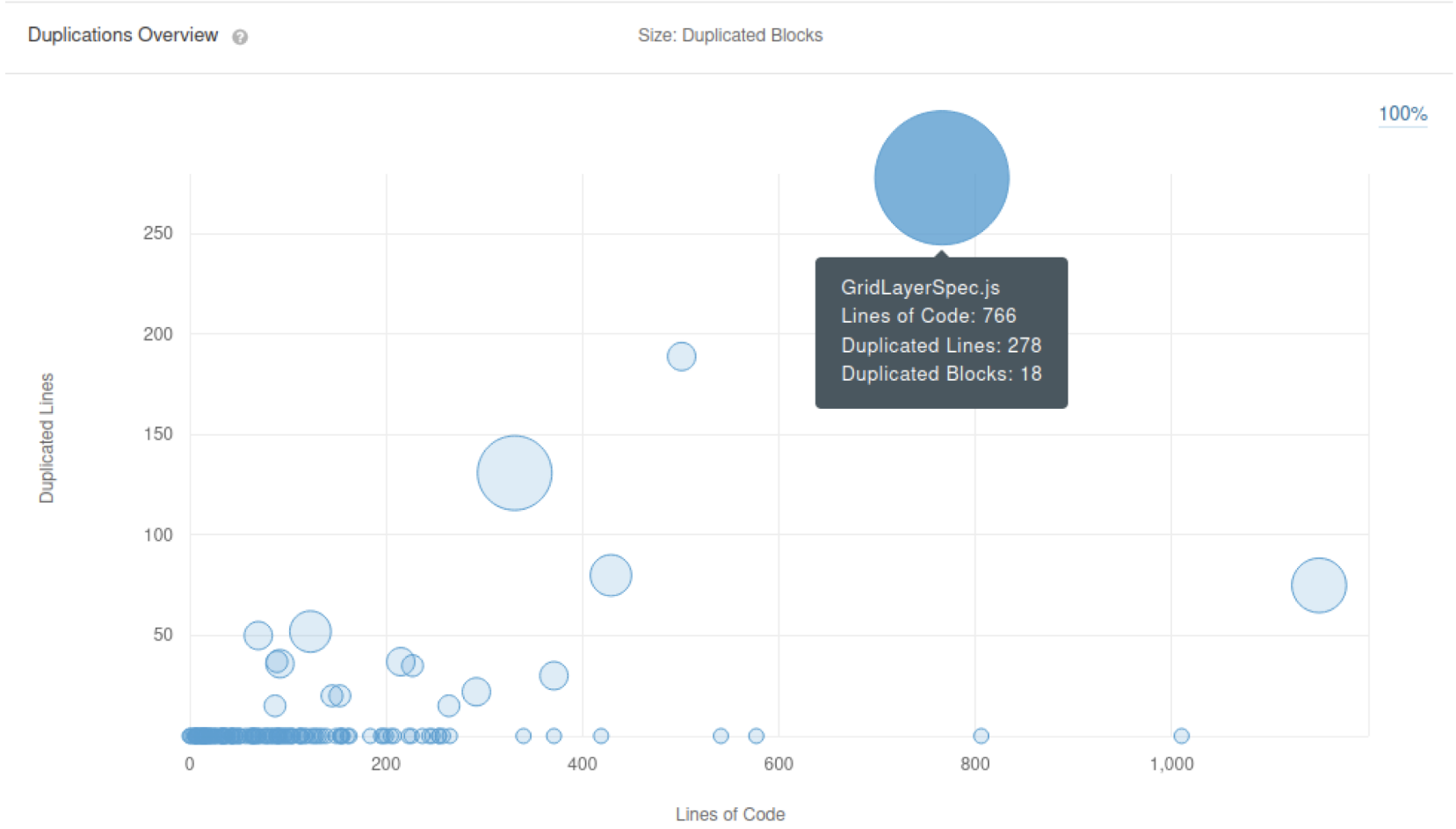
Get Permalink

```
114  // `false` can be passed to skip any processing (can be useful to avoid round-off errors).
115  export function formatNum(num, precision) {
116      if (precision === false) { return num; }
117      var pow = Math.pow(10, precision === undefined ? 6 : precision);
118      return Math.round(num * pow) / pow;
119  }
120
121  // @function trim(str: String): String
122  // Compatibility polyfill for [String.prototype.trim](https://developer.mozilla.org/docs/Web/JavaScript/Reference/Global_Objects/String
     /Trim)
123  export function trim(str) {
124      return str.trim ? str.trim() : str.replace(/^\s+|\s+$/g, '');
```

Make sure the regex used here, which is vulnerable to super-linear runtime due to backtracking, cannot lead to denial of service. Comment

Automatische statische Analyse
Duplications (4%)

Brandenburgische Technische Universität Cottbus



Automatische statische Analyse
Duplications (4%)

Brandenburgische Technische Universität Cottbus

Duplicated Lines (%) **4.0%**

	Duplicated Lines (%)	Duplicated Lines
spec/suites/geo/projection/ProjectionSpec.js	51.0%	50
spec/suites/layer/vector/PathSpec.js	33.6%	37
spec/suites/map/handler/Map.TouchZoomSpec.js	32.3%	52
spec/suites/map/handler/Map.DragSpec.js	31.3%	131
spec/suites/layer/marker/Marker.DragSpec.js	30.8%	36
spec/suites/dom/DomEventSpec.js	28.3%	189
spec/suites/layer/tile/GridLayerSpec.js	25.1%	278
spec/suites/layer/PopupSpec.js	14.9%	80
spec/suites/layer/vector/PolylineSpec.js	13.2%	37
spec/suites/layer/vector/RectangleSpec.js	13.2%	15
spec/suites/layer/vector/CanvasSpec.js	12.8%	35
spec/suites/geometry/BoundsSpec.js	11.3%	20
spec/suites/geo/LatLngBoundsSpec.js	10.6%	20
spec/suites/control/Control.LayersSpec.js	6.1%	22
spec/suites/layer/TooltipSpec.js	6.1%	30
spec/suites/map/MapSpec.js	5.4%	75
spec/suites/layer/vector/PolygonSpec.js	4.3%	15

Automatische statische Analyse
Zusammenfassung

Brandenburgische Technische Universität Cottbus

Lines of Code	19211
Lines	28324
Statements	11514
Functions	2612
Files	144
Comment Lines	4116
Comment(%)	17.6%
Duplicated Lines	1122
Duplicated(%)	4%
Cyclomatic Complexity	4373
Cognitive Complexity	2202

Automatische statische Analyse
Zusammenfassung

Brandenburgische Technische Universität Cottbus

	Lines of Code	Bugs	Vulnerabilities	Code Smells	Security Hotspots	Coverage	Duplications
Leaflet-js							
└ build	88	0	0	11	0	0.0%	0.0%
└ debug/vector	50	0	0	1	0	0.0%	0.0%
└ docs	394	1	0	36	0	0.0%	0.0%
└ spec	10,289	4	0	1,381	0	0.0%	8.6%
└ src	8,390	2	0	769	5	0.0%	0.0%