Fix prototype pollution vulnerability (#77)

Browse files

```
* Fix prototype pollution vulnerability

* Fix test
```

master (#77)
v2.1.4

diegohaz committed on Mar 12, 2020 1 parent fecef6e commit 1987fefcb3b7508253a29502a008d5063a873cef

Showing **4 changed files** with **25 additions** and **3 deletions**.

Split Unified

3 .travis.yml

```
@@ -1,7 +1,6 @@
 language: node_js
 services: mongodb
 node_js:
-  - v5
-  - v4
+  - v6
 after_script:
   - 'npm run coveralls'
```

8 src/index.js

```
   * @param {Function} [fn] - Set the handler method.
   */
  export function handler (type, name, fn) {
+   if (
+     type === 'constructor' ||
+     type === '__proto__' ||
+     name === 'constructor' ||
+     name === '__proto__'
+   ) {
+     return
+   }
    if (arguments.length > 2) {
      handlers[type][name] = fn
    }
```

15 test/index.js

```
    return app
  }

+ test('Prototype pollution', (t) => {
+   const { toString } = {}
+
+   querymen.handler('__proto__', 'toString', 'JHU')
+   t.ok({}.toString === toString, 'should not be vulnerable to prototype pollution')
+
+   querymen.handler('formatters', '__proto__', { toString: 'JHU' })
+   t.ok({}.toString === toString, 'should not be vulnerable to prototype pollution')
+
+   querymen.handler('validators', '__proto__', { toString: 'JHU' })
+   t.ok({}.toString === toString, 'should not be vulnerable to prototype pollution')
+
+   t.end()
+ })
+
  test('Querymen handler', (t) => {
    t.notOk(querymen.parser('testParser'), 'should not get nonexistent parser')
    t.notOk(querymen.formatter('testFormatter'), 'should not get nonexistent formatter')
```

2 test/querymen-schema.js

```
    t.same(add('123,456', [Number]), [123, 456], 'should add a param with type option number array')
    t.same(add('123,0', [Boolean]), [true, false], 'should add a param with type option boolean array')
    t.same(add('2016,2017', [Date]), [new Date('2016'), new Date('2017')], 'should add a param with type option date array')
-   t.same(add('123,456', [RegExp]), [/123/i, /123/i], 'should add a param with type option regexp array')
+   t.same(add('123,456', [RegExp]), [/123/i, /456/i], 'should add a param with type option regexp array')
    t.end()
  })
```

0 comments on commit `1987fef`

Please sign in to comment.