PA193 Project: Part 3 Report

Code Review

Lenka Bačinská Ondřej Koutský Lukáš Němec

10.12. 2013

Contents

1 Reviewed project **2**

2 Checks and errors **2**

2.1 Pugixml 2

2.2 Svg tag attributes 3

2.3 Attribute not allowed in concrete tag 3

1 Reviewed project

Program we were reviewing is SVG parser. It takes one command line argument (name of the SVG file) as input.

This file must have valid XML structure. It must contain tag `svg`. As children of this tag three shapes are supported: circle, ellipse and rectangle. Supported attributes are:

- `circle`: `r` (mandatory), `cx`, `cy`
- `ellipse`: `rx` (mandatory), `ry` (mandatory), `cx`, `cy`
- `rect`: `width` (mandatory), `height` (mandatory), `x`, `y`, `rx`, `ry`
- optional for all shapes: `stroke`, `opacity`, `fill`, `fill-opacity`, `stroke-opacity`, `stroke-width`

2 Checks and errors

First thing we did was checking the code with cppcheck and PreFast analysers. Both of them found some warnings (and one error) in the used external library *pugixml*. So at first we focused on this.

Second thing was manual code review, where we found two problems. `svg` tag attributes are not checked and wrong decision about input correctness when the allowed attribute is used in SVG shape, where it doesn't belong.

We were not able to find any others mistakes and vulnerabilities. The regular expressions used are very well done, they are "bullet-proof".

2.1 Pugixml

External library *pugixml* used to find out, if the given file is correct XML doesn't check, if there is only one main tag. Parser then parses only children of `svg` tag, so anything behind is allowed, although it shouldn't be.

Input

```
<svg xmlns="http://www.w3.org/2000/svg" version="1.1">
</svg>
<Tag attr="We got you!" />
```

Output

```
Filename: svgfile.svg
Succcessfully checked attributes:
Everyhing ok:)
```

There may be more vulnerabilities caused by this library, but we didn't try to find them. It would be still the same mistake - usage of the vulnerable external code.

2.2 Svg tag attributes

The program is not checking the attributes in the `svg` tag. We think, this is a big error, at least names of the attributes should be checked.

Input

```
<svg look="We got you!">
</svg>
```

Output

```
Filename: svgfile.svg
Succcessfully checked attributes:
Everyhing ok:)
```

2.3 Attribute not allowed in concrete tag

There are attributes, that are allowed in some tags, but not all. The program checks it, but still the result is "Everything ok".

Input

```
<svg xmlns="http://www.w3.org/2000/svg" version="1.1">
    <circle cx="1" cy="1" r="1" x="5"/>
</svg>
```

Output

```
Filename: svgfile.svg
Succcessfully checked attributes:
circle:  cx=1 cy=1 r=1
Error: element "circle" has invalid attribute "x"
 x=5
Everyhing ok:)
```