Lookup Editor - Bug #2839

jexcel fails on XSS

07/17/2020 05:29 AM - Luke Murphey

Status:	Closed	**Start date:**	07/17/2020
Priority:	Normal	**Due date:**	
Assignee:	Luke Murphey	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	3.4.6		

Description

Associated revisions

Revision 671 - 07/17/2020 02:38 PM - luke.murphey

Updating jexcel to fix XSS issue

Closes #2839

History

#1 - 07/17/2020 05:45 AM - Luke Murphey

Obs:

- I am using updateTable() to override the cell values.
- The cell contents are getting executed before my render even gets called.
- This line is where the issue is coming from:

```
        // Append nodes to the HTML
        for (j = 0; j < obj.options.data.length; j++) {
            // Create row
            var tr = obj.createRow(j, obj.options.data[j]);
            // Append line to the table
            if (j >= startNumber && j < finalNumber) {
                obj.tbody.appendChild(tr);
            }
        }
```

Qs:

- Where is the XSS getting executed?
  - Just passing the data causes this
- Does jexcel have some sort of XSS protection I ought to be enabling?
  - https://github.com/paulhodel/jexcel/issues/959
- Can I disable formulas?
  - https://github.com/paulhodel/jexcel/issues/102
- Does it work if I remove my custom renderer?
  - No, my custom renderer was actually improving things somehow
- Does removing custom columns help?
  - Nope
- Does 4.0 have this issue?
  - Cannot get it loaded

#2 - 07/17/2020 02:24 PM - Luke Murphey

Jexcel 4 doesn't load: Module name "jsuites/dist/jsuites.css" has not been loaded yet for context: _. Use require([])

Qs:

- Why is the module named "jsuites/dist/jsuites.css"? I don't have it under dist
- Why is it complaining for _"

Obs:

- jsuites is trying to load it:

```
if (! jSuites && typeof(require) === 'function') {
    var jSuites = require('jsuites');
    require('jsuites/dist/jsuites.css');
```

Solns:

- Put jexcel in a require("jexcel") call
  - Nope
- Move jsuites under jexcel directory
- Remove jsuites css require call
  - This fixed it

Refs:

- https://requirejs.org/docs/errors.html#notloaded

#3 - 07/17/2020 02:39 PM - Luke Murphey

- Status changed from New to Closed

- Target version set to 3.4.6

- % Done changed from 0 to 100