AllenFang / react-bootstrap-table Public

<> Code Issues 422 Pull requests 20 Actions Projects Wiki ···

New issue

Jump to bottom

XSS when using dataFormat function #2071

Open **michaelrodov** opened this issue on Apr 18, 2019 · 2 comments

michaelrodov commented on Apr 18, 2019 • edited

Hi
When using dataFormat function and not converting the value to react component
output is not sanitised. Therefore you can easily run XSS through it.

```
const Demo = props => {
  let data = [
    {key: "1", value: "test"},
    {key: "2", value: '/1337"><noscript><p title="</noscript><img src=x onerror=alert`openbugbounty`>">'}
  ]
  return (
      <BootstrapTable data={data}>
        <TableHeaderColumn dataField="key" isKey />
        <TableHeaderColumn dataField="value" dataFormat={v => v} />
      </BootstrapTable>
  );
};
```

Example: https://codesandbox.io/s/q7oj2v6xo9?fontsize=14

oeph commented on May 10, 2021

It is caused by

react-bootstrap-table/src/TableBody.js
Lines 114 to 118 in `26d07de`

```
114       if (!React.isValidElement(formattedValue)) {
115         columnChild = (
116           <div dangerouslySetInnerHTML={ { __html: formattedValue } }></div>
117         );
118       } else {
```

If you return a invalid react element, it will use `dangerouslySetInnerHTML` . Your fix could be to use the following `dataFormat` :
`dataFormat={v => (<span>{v}</span>)}`

eborden commented on Dec 22, 2021

There is now a CVE pointing at this issue. Are there plans to fix this XSS exploit?

GHSA-2589-w6xf-983r

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants