./ chris-forbes.github.io

View on GitHub

CVE-2021-31792

As part of my ongoing hobbiest information security research I came across an XSS in the opensource SuiteCRM customer relationship management webapp, developed by Sales Agility.

There is a bug in the input validation of the name field of the client account page.

Accounts page bugs

Javascript injection bug:

The following javascript attribute can be injected into the name field, then click the tick and mouse over the function call

```
" onmouseover=Function`alert\x28document.cookie\x29```
```

Overwrite bug:

The javascript gets sanitised properly when the page is reloaded however you can re-active it with a secondary bug on on the form.

1. Double click the website field to edit it
2. without saving the field, double click on email address to edit it and click ok at the popup
3. the data from the name field will now overflow and be duplicated in the email field, both of which will now execute the injection above