New issue

Jump to bottom

XSS vulnerability #2917

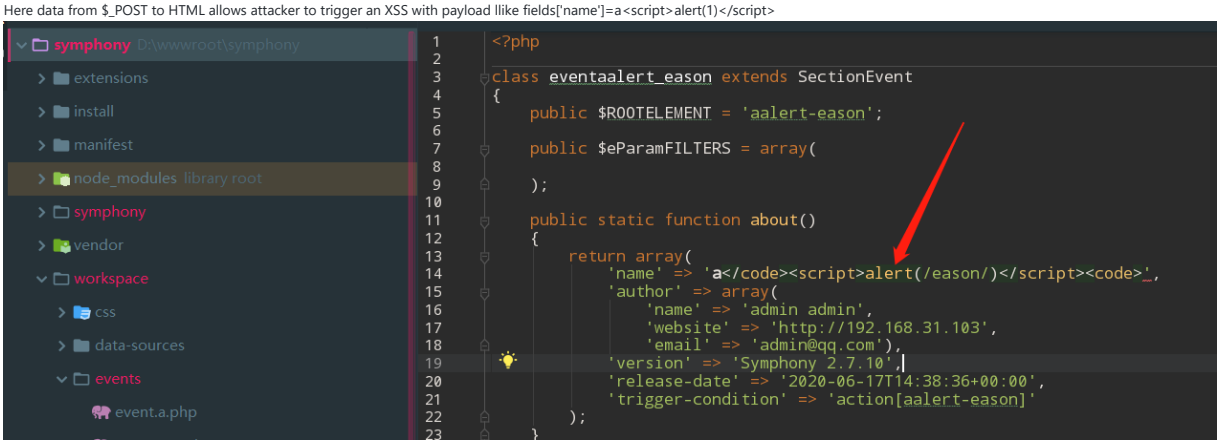
Open 3as0n opened this issue on Jun 17, 2020 · 1 comment

3as0n commented on Jun 17, 2020

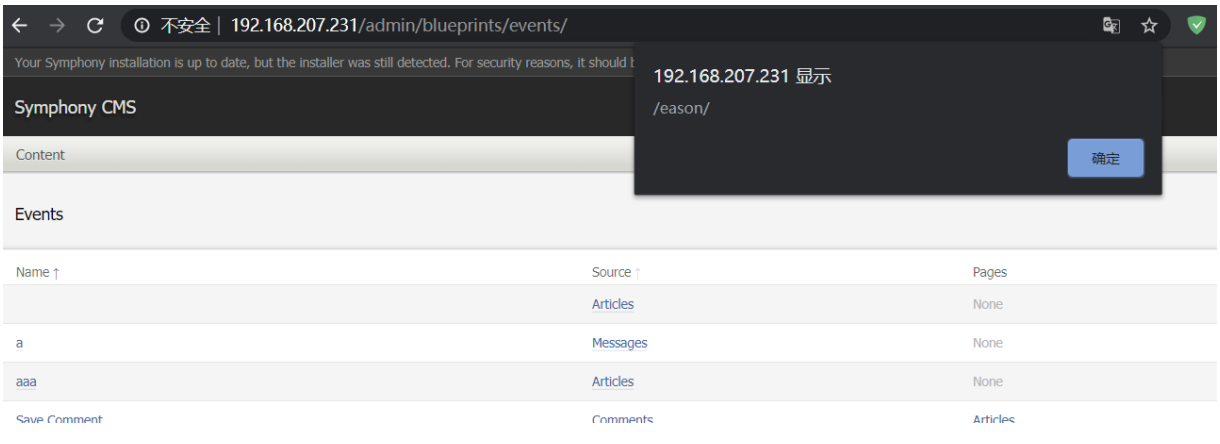
https://github.com/symphonycms/symphonycms/blob/master/symphony/content/content.blueprintsevents.php

```
$about = General::array_map_recursive('stripslashes', $existing->about());
....
....
....
$this->appendSubheading(($isEditing ? $about['name'] : __('Untitled')))
....
....
....


  public function appendSubheading($value, $actions = null)
    {
        if (!is_array($actions) && $actions) { // Backward compatibility
            $actions = array($actions);
        }

        if (!empty($actions)) {
            foreach ($actions as $a) {
                $this->insertAction($a);
            }
        }

        $this->Breadcrumbs->appendChild(new XMLElement('h2', $value, array('role' => 'heading', 'id' => 'symphony-subheading')));
    }
```

Here data from $_POST to HTML allows attacker to trigger an XSS with payload like fields['name']=a<script>alert(1)</script>



3as0n commented on Jun 17, 2020 Author



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant