New issue

Jump to bottom

XSS in admin dashboard #51

Closed **b1nslashsh** opened this issue on Nov 29, 2020 · 3 comments

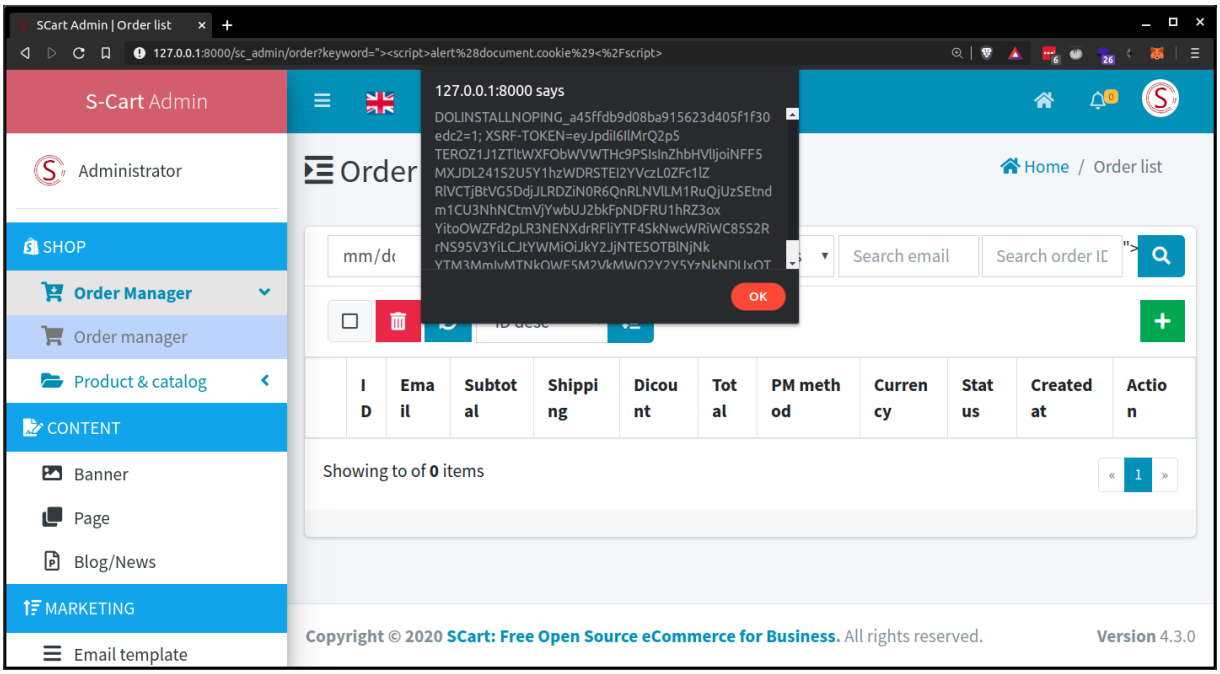
b1nslashsh commented on Nov 29, 2020 • edited

Reflected xss in admin panel
There is a cross site scripting or xss in admin Dashboard

To Reproduce

1. the search function in admin dashboard is vulnerable for XSS
   https://demo.s-cart.org/sc_admin/order?keyword=%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E

Screenshots



Fix for it :)

Useing htmlentities() in s-cart/core

https://github.com/s-cart/core/blob/master/src/Admin/Controllers/AdminOrderController.php#L170
will fix this issue

```
<option value="">Search order status</option>
<option value="1">New</option><option value="2">Processing</option><option value="3">Hold</option><option value="4">Canceled</option><option value="5">Done</option><op
</select>
</div>  
<input type="text" name="email" class="form-control rounded-0 float-right" placeholder="Search email" value="">  
<input type="text" name="keyword" class="form-control rounded-0 float-right" placeholder="Search order ID" value="&quot;&gt;&lt;script&gt;alert(document.cookie)&lt;/script&gt;">
<div class="input-group-append">
<button type="submit" class="btn btn-primary"><i class="fas fa-search"></i></button>
</div>
iv>
```

1

lanhktc commented on Nov 29, 2020 • edited — Collaborator

Thanks so much. This error will fix in the next release

lanhktc commented on Dec 5, 2020 — Collaborator

Fixed in SC 4.4

lanhktc closed this as completed on Dec 5, 2020

abergmann commented on Dec 16, 2020

CVE-2020-28457 was assigned to this issue.

1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants