grocy / **grocy** Public

Code · **Issues** 148 · Pull requests 2 · Security 1 · Insights

New issue

Jump to bottom

XSS and HTML Injection on Create Shopping List & shopping list item notes (Rendered upon deleting it) #996

Closed **muffyhub** opened this issue on Sep 8, 2020 · 7 comments

Labels bug

Milestone v3.0.0

muffyhub commented on Sep 8, 2020 • edited by berrnd

Edit by @berrnd:

Just to note that here:
I don't consider this critical for grocy, this cannot be done unauthenticated, grocy is not an application you (should) host publicly (means without authentication) on the internet.

Vulnerability Name: Stored Cross Site Scripting & HTML Injection

Vulnerability Description: grocy household management solution v2.7.1, allows stored XSS and HTML Injection, via Create Shopping List module, that is rendered upon deletiing that Shopping List.
Cross Site Scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to the web application. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.
HTML injection occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page. Consequences can be disclosure of a user's session cookies that could be used to impersonate the victim, or, more generally, it can allow the attacker to modify the page content seen by the victims.

Vulnerable URL: http://127.0.0.1/shoppinglist/new

Payload:

```
1. <marquee onstart=alert(document.cookie)>
2. <h1>HTML Injection</h1>
```

Steps to Reproduce:

1. Login to the application
2. Go to 'Shooping List' module
3. Click on 'New Shopping List' module
4. Enter the payload: in 'Name' input field.
5. Click Save
6. Click 'Delete Shopping List'
   Request:
   POST /api/objects/shopping_lists HTTP/1.1
   Host: 127.0.0.1
   User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
   Accept: /
   Accept-Language: en-US,en;q=0.5
   Accept-Encoding: gzip, deflate
   Referer: http://127.0.0.1/shoppinglist/new
   Content-type: application/json
   Content-Length: 38
   Connection: close
   Cookie: grocy_session=GhIjKZySST7Qkx18Q97u9MaPM1LsMtBmcJ6I59gxTO3Ks4WJXUd
   {"name":" "}

berrnd mentioned this issue on Sep 8, 2020

XSS possibilty on shopping list page #991
Closed

berrnd added the **ui-bug** label on Sep 8, 2020

berrnd added this to the **v3.0.0** milestone on Sep 8, 2020

berrnd commented on Sep 8, 2020 • edited · Member

Merged #991 into this.

So this also affects shopping list item notes.

berrnd changed the title ~~XSS and HTML Injection on Create Shopping List (Rendered upon deleting it)~~ **XSS and HTML Injection on Create Shopping List & shopping list item notes (Rendered upon deleting it)** on Sep 8, 2020

fipwmaqzufheox... commented on Sep 8, 2020 • edited · Contributor

I can reproduce this also on: users, batteries, chores, equipment, locations, quantity units, shopping locations, tasks, taskcategories, product groups, recipes, products

(For all: add an item named `<marquee onstart=alert(document.cookie)>` , save and try to delete it)

For recipes: you can also use a product named `<marquee onstart=alert(document.cookie)>` as ingredient and delete it from the ingredient list (or an included recipe named so)

fipwmaqzufheox... commented on Sep 8, 2020 Contributor

via API or JS-Console:
`Grocy.Api.Put('objects/shopping_lists/1', {"description":" <marquee onstart=alert(document.cookie)> "})`
and then open the shopping list
or
`Grocy.Api.Put('objects/recipes/2', {"description":" <marquee onstart=alert(document.cookie)> "})`
and then open the recipe (in recipes list or in recipe form)

Create a userfield, e.g. for products, use USERFIELD_TYPE_PRESET_CHECKLIST (= "Select list (multiple items can be selected)"), add `<marquee onstart=alert(document.cookie)>` as value, choose "Show in tables", and then edit any product, check the field, and open the stockoverview

berrnd added a commit that referenced this issue on Sep 8, 2020

`Excape HTML (where needed, for bootbox) (references #996)` 0df2590

berrnd added a commit that referenced this issue on Sep 8, 2020

`Excape shopping list item notes (references #996)` 0624b0d

berrnd commented on Sep 8, 2020 • edited Member

I fixed some parts of the mentioned places, see the referenced commits above. Maybe filtering the input before saving it (so mostly in the "Generic entity interactions" API routes") would be better...

berrnd added a commit that referenced this issue on Oct 14, 2020

`Sanitize user input on all API routes (references #996)` c110014

berrnd added a commit that referenced this issue on Oct 14, 2020

`Revert "Excape HTML (where needed, for bootbox) (references #996)"` … 08644f9

berrnd added a commit that referenced this issue on Oct 14, 2020

`Added changelog for #996` 56d79d7

berrnd commented on Oct 14, 2020 Member

I think this should now be resolved, I've added fiiltering of the whole request body for all API routes in `c110014` .

Feel free to play around with it on the pre-release demo and let me know here if you find any other/leftover places where this is still possible.

berrnd closed this as completed on Oct 14, 2020

kriddles commented on Oct 14, 2020 Contributor

> I think this should now be resolved, I've added fiiltering of the whole request body for all API routes in c110014.
>
> Feel free to play around with it on the pre-release demo and let me know here if you find any other/leftover places where this is still possible.

Not sure if it's related but on the pre-release demo I cannot edit stock entries anymore.

berrnd mentioned this issue on Oct 15, 2020

Stock entries cannot be edited (current master) #1055

Closed

berrnd commented on Oct 15, 2020 Member

> Not sure if it's related but on the pre-release demo I cannot edit stock entries anymore.

Maybe, I added to use htmlpurifier to just filter all request body properties (code ref), so maybe this breaks/removes something which is not "bad HTML"...

Moved this to #1055.

berrnd added a commit that referenced this issue on Oct 17, 2020

`Don't strip boolean values (references #996, fixes #1055)` 5ed7a0c

This was referenced on Dec 29, 2020

UI-Bug: Images in equipment descriptions #1228

Closed

Bug: Ampersand (&) in name field is converted to HTML entity #1247

Closed

berrnd added bug and removed ui-bug labels on Jul 3, 2021

berrnd mentioned this issue on Oct 5, 2021

Potential security issue #1643

Closed

Assignees

No one assigned

Labels

bug

Milestone

v3.0.0

Development

No branches or pull requests

4 participants