

New issue

Jump to bottom

## Security Fix for Cross-site Scripting (XSS) - huntr.dev #4543

**Closed** huntr-helper wants to merge 9 commits into `monica:master` from `418sec:2-other-monica`

Conversation 9 Commits 9 Checks 0 Files changed 5



huntr-helper commented on Oct 12, 2020

<https://huntr.dev/users/alromh87> has fixed the Cross-site Scripting (XSS) vulnerability. alromh87 has been awarded \$25 for fixing the vulnerability through the huntr bug bounty program. Think you could fix a vulnerability like this?

Get involved at <https://huntr.dev/>

Q | A

Version Affected | ALL

Bug Fix | YES

Original Pull Request | [418sec#2](#)

Vulnerability README | <https://github.com/418sec/huntr/blob/master/bounties/other/monica/2/README.md>

### User Comments:

#### Metadata \*

Bounty URL: <https://www.huntr.dev/bounties/2-other-monica>

#### Description \*

XSS queries being triggered from people info page by the audit log at the settings, fix sanitizes content before showing to user.

#### Technical Description \*

Even though Laravel has inbuilt protection for XSS it has been disabled when presenting log: `{!! $log['description'] !!}` to enable embedding contact links, leading to XSS, htmlentities was used to sanitize data before showing to user, effectively avoiding new as well as already stored XSS.

#### Edit

Looking further into the code I realized the XSS protection have been disabled in many views so I added a Middleware that will strip html tags using `strip_tags`, and since `strip_tags` can be tricked with malformed markup remaining input is encoded using htmlentities.

Middleware is at `app/Http/Middleware/SanitizeInput.php` and can be tuned for specific keys adding them to the `$except` array:

```
/**
 * The names of the attributes that should not be trimmed.
 *
 * @var array
 */
protected $except = [
    'password',
    'password_confirmation',
    '_token',
    ''
];
```

#### Proof of Concept (PoC) \*

1. Download and setup monica
2. Create new contact, introducing payload as name:  
`<svg/onload=alert("firstname1")><script> alert("firstname2_xss")</script> <script> alert("midname_xss")</script> <script> alert("lname_xss")</script><svg/onload=alert(1)>(<svg/onload=alert("nickie1")>)`
3. Go to Settings -> Audit logs
4. XSS is triggered

localhost:8081/settings/auditlogs

localhost:8081 dice  
midname\_xss

Panel de control Contactos Diario

Panel de control > Ajustes > Usuarios

Configuración de cuenta

Personalización

Almacenamiento

Exportar datos

Importar datos

Usuarios

Administrar tags

API

Descargue P&V

Everything that happened to this account

Added

After fix introduced data is displayed as text and no XSS is executed

Stored XSS will be also stripped out and encoded after contact is edited

## User Acceptance Testing (UAT)

Functionality is unaffected, contact link works as usual

localhost:8081/people/h:4G7r3K91nkYn2LWe5m\_load=alert("firstname1")><script> alert("firstname2\_xss")

-O-	Merge pull request #1 from Mik317/master ...	✗ a80858d
-O-	Merge branch 'master' into master	✗ 098e345
-O-	[FIX] Stored-XSS using htmlentities() in audit log	4e2b8d1
-O-	Filter also when no user	c9b516c
-O-	Fix XSS ...	4651b45
-O-	Fix XSS (Clean up)	58b4a03
-O-	Merge pull request #2 from alromh87/master ...	✗ 0764eba

CLAAssistant commented on Oct 12, 2020 • edited

CLA not signed yet

Thank you for your submission! We really appreciate it. Like many open source projects, we ask that you all sign our [Contributor License Agreement](#) before we can accept your contribution. 4 out of 5 committers have signed the CLA.

☒ Mik317  
☒ alromh87  
☒ JamieSlome  
☒ asbiin  
☒ Raj

Raj seems not to be a GitHub user. You need a GitHub account to be able to sign the CLA. If you have already a GitHub account, please [add the email address used for this commit to your account](#). You have signed the CLA already but the status is still pending? Let us [recheck](#) it.

JamieSlome commented on Oct 12, 2020

@alromh87 - are you able to sign the CLA? Let me know if you have any questions! 🍷

👍 1 🗨️ 1

alromh87 commented on Oct 12, 2020

Sure 😊

asbiin commented on Oct 15, 2020

Member

Hi @huntr-helper @JamieSlome @alromh87  
 Thank you for your submit.  
 However, I cannot merge this change.  
 htmlentities is not to be used directly, as Laravel already handle this kind of security checks (but I don't know yet why it's not doing it in this case).  
 Anyway, if you want to consider it, please remove the first changes done in the commit [3871537](#), because it has been superseded by another fix [here](#).

alromh87 commented on Oct 15, 2020

I will update tomorrow, I found in many places protection was disabled due to using {!! \$log['description'] !!}

🗨️ alromh87 mentioned this pull request on Oct 16, 2020

Removed use of htmlentities as requested by maintainer 418sec/monica#3

➡ Merged

alromh87 commented on Oct 16, 2020

@asbiin Updated as per requested and updated with upstream, use of htmlentities was removed when presenting information, only middleware for sanitizing before storage is preserved.

-O- Merge branch 'master' into 2-other-monica

✗ c7ed798

asbiin commented on Dec 9, 2020

Member

@alromh87 any update on that fix? Current changes still uses htmlentities(), and it should never been required.

🔖 asbiin added the waiting for answers label on Dec 12, 2020

🗨️ RMHogervorst mentioned this pull request on Feb 18, 2021


Security Issue - XSS #4888

🔒 Closed

asbiin commented on Mar 1, 2021

Member

This PR has been on hold for a long time.  
 I'll close it for now, don't hesitate to reopen if needed.

 asbiin closed this on Mar 1, 2021

github-actions  commented on Mar 1

This pull request has been automatically locked since there has not been any recent activity after it was closed. Please open a new issue for related bugs.

 github-actions  locked as resolved and limited conversation to collaborators on Mar 1

Reviewers

No reviews

Assignees

No one assigned

Labels

**waiting for answers**

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

6 participants

