

New issue

[Jump to bottom](#)

Stored XSS #1660

🔒 Closed

delyura opened this issue on Aug 30 · 4 comments

Assignees



Labels

Bug

Milestone

🏠 Siena 0.9.21

delyura commented on Aug 30

Hello, we found the stored xss.
Tested on latest version 0.9.20.
Poc:

1. Write a DM to any user

84.201.175.126/Cotonti/index.php?e=pm&m=send&to=1

Главная
start here

Форумы
discussions

News
our updates

RSS
subscribe me

Личные сообщения / Новое личное сообщение

Форма для создания нового сообщения

Входящие сообщения / Отправленные сообщения / Создать новое сообщение

Получатели:

admin

до 10 получателей, разделенных запятыми

Тема:

Stored XSS

Сообщение:

✂

📄

🗑

🔖

📁

🔍

ABC

↶

↷

🔍

🌐

📝

⌨

🔗

🔄

📱

📧

☺

Ω

➡

🔄

📋

🔗

Источник

?

B

I

U

~~S~~

x₂

x^p

≡

≡

≡

≡

”

☰

☰

☰

☰

🔗

💬

🚩

...

{ }

Code

Стили ▾ | Обычное ▾ | A ▾ A ▾


"<script>alert(document.cookie)</script>

body p

☐ Не сохранять в исходящих

Отправить

2. Then read the incoming message and press "quote" to quote the message with payload. Press the button Response.

 Alex300 self-assigned this on Aug 31

  Alex300 added **Critical** **Bug** labels on Aug 31



  Alex300 added this to the **Siena 0.9.21** milestone on Aug 31

Alex300 commented on Sep 4

Member

Same as [#1661](#). This thing is available only to administrators. This is related to the HTML Purifier settings. Administrators have more permissions than regular users.

It is needed to disable JavaScript in HTMLPurifier somehow for admins too.

  Alex300 removed the **Critical** label on Sep 4

 Alex300 added a commit that referenced this issue on Sep 4


 Fix for [#1660](#), [#1661](#) ...

41f7516

Alex300 commented on Sep 4

Member

`<script>` tags are disabled in HTMLPurifier for admins too

 Alex300 closed this as completed on Sep 4

delyura commented on Sep 4

Author

`<script>` tags are disabled in HTMLPurifier for admins too

Creating blacklists is not best practice, you should use whitelist. For example, you disable the `<script>` tag, but the payload `` will work.

For a comprehensive list, check out the [DOMPurify allowlist](#).

Alex300 commented on Sep 4

Member

see here: [#1661](#)

Assignees

 Alex300

Labels

Bug

Projects

None yet

Milestone

Siena 0.9.21

Development

No branches or pull requests

2 participants

