Cotonti / **Cotonti** Public

Code · **Issues** 91 · Pull requests · Actions · Projects · Security · ...

New issue

Jump to bottom

Stored XSS on forum #1661

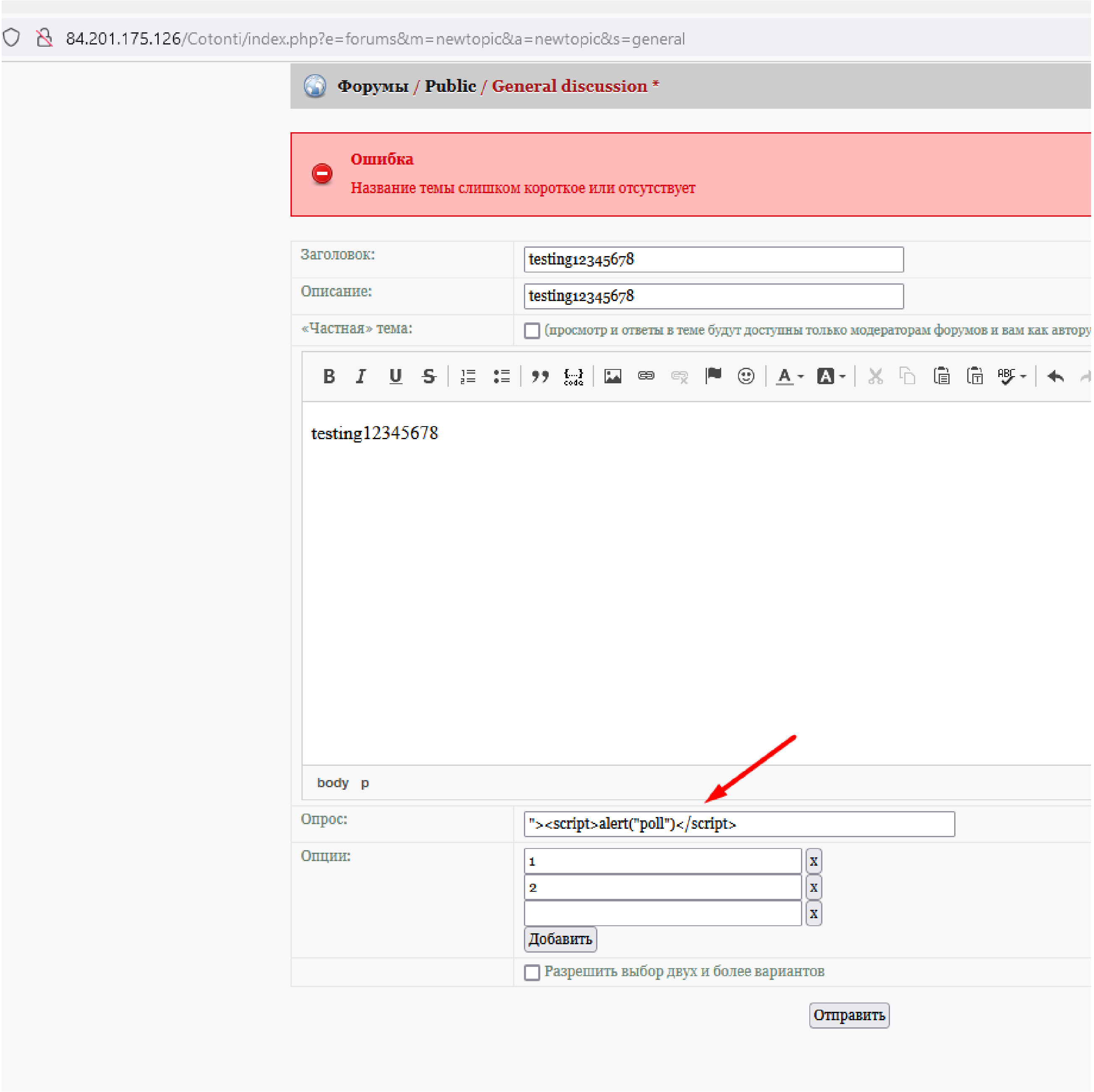
Closed **delyura** opened this issue on Aug 30 · 6 comments

Assignees	
Labels	Bug
Milestone	Siena 0.9.21

delyura commented on Aug 30

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

1. Create new topic with poll



84.201.175.126/Cotonti/index.php?e=forums&m=newtopic&a=newtopic&s=general

Форумы / Public / General discussion *

Ошибка

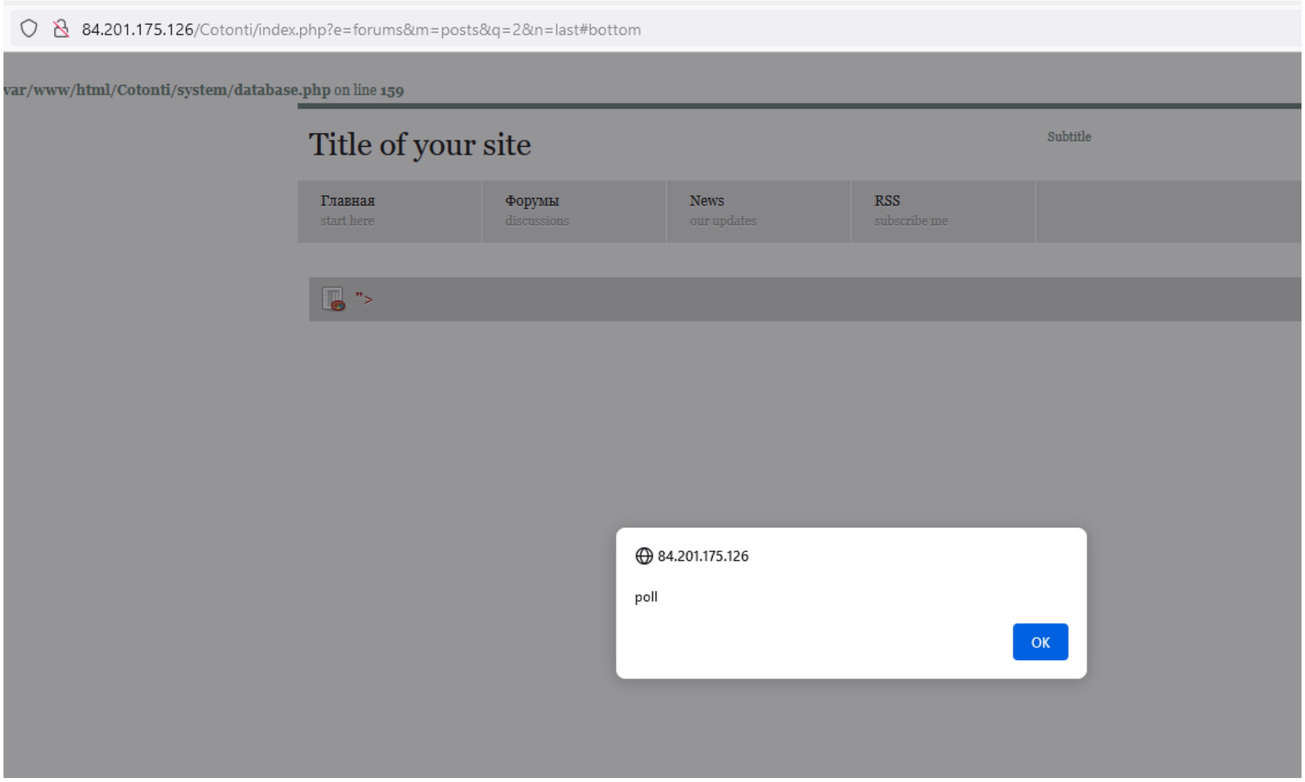
Название темы слишком короткое или отсутствует

Заголовок:	testing12345678
Описание:	testing12345678
«Частная» тема:	□ (просмотр и ответы в теме будут доступны только модераторам форумов и вам как автору

testing12345678

Опрос:	"><script>alert("poll")</script>
Опции:	1 x 2 x x Добавить
	□ Разрешить выбор двух и более вариантов

2. XSS execute



84.201.175.126/Cotonti/index.php?e=forums&m=posts&q=2&n=last#bottom

var/www/html/Cotonti/system/database.php on line 159

poll

Alex300 added Critical Bug labels on Aug 31

Alex300 self-assigned this on Aug 31

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

Alex300 commented on Sep 4 • edited ▾ Member

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 mentioned this issue on Sep 4

Stored XSS #1660

Closed

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

👍 1

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 `<img src=x onerror=alert(1)>` will work.
For a comprehensive list, check out the DOMPurify allowlist.

Alex300 commented on Sep 4 Member

Are you suggesting to make a whitelist with all possible valid options, except for the <script> tag :)?

> but the payload `<img src=x onerror=alert(1)>`

Really? I can't reproduce this case.

Moreover, this situation is only possible if administrator will save text with the XSS script. Regular users has more stricter HTMLPurifier settings.

Cristian-Bejan commented on Sep 8

> Are you suggesting to make a whitelist with all possible valid options, except for the <script> tag :)?
>
> > but the payload `<img src=x onerror=alert(1)>`
>
> Really? I can't reproduce this case.
>
> Moreover, this situation is only possible if administrator will save text with the XSS script. Regular users has more stricter HTMLPurifier settings.

He is saying to **only allow** (whitelist) e.g. plain text. Thus you will automatically reject everything else.

Alex300 commented on Sep 8 Member

I understood, but in this case it is needed all options from HTMLPurifier default policy except JS tag and attributes)

👍 1

Assignees

Alex300

Labels

Bug

Projects

None yet

Milestone

Siena 0.9.21

Development

No branches or pull requests

3 participants