joinia Update 1.md History

1 contributor

28 lines (13 sloc) | 772 Bytes

Htmly Authenticated Stored Cross-Site Scripting(XSS)

Description

Htmly CMS does not filter the content correctly at the "edit profile" module, resulting in the generation of stored XSS.

Affects CMS

Htmly CMS

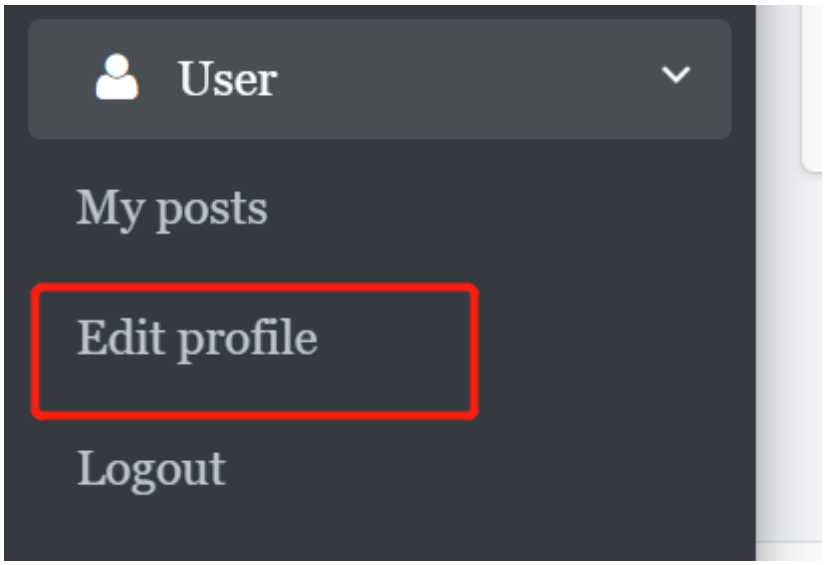
https://github.com/danpros/htmly/

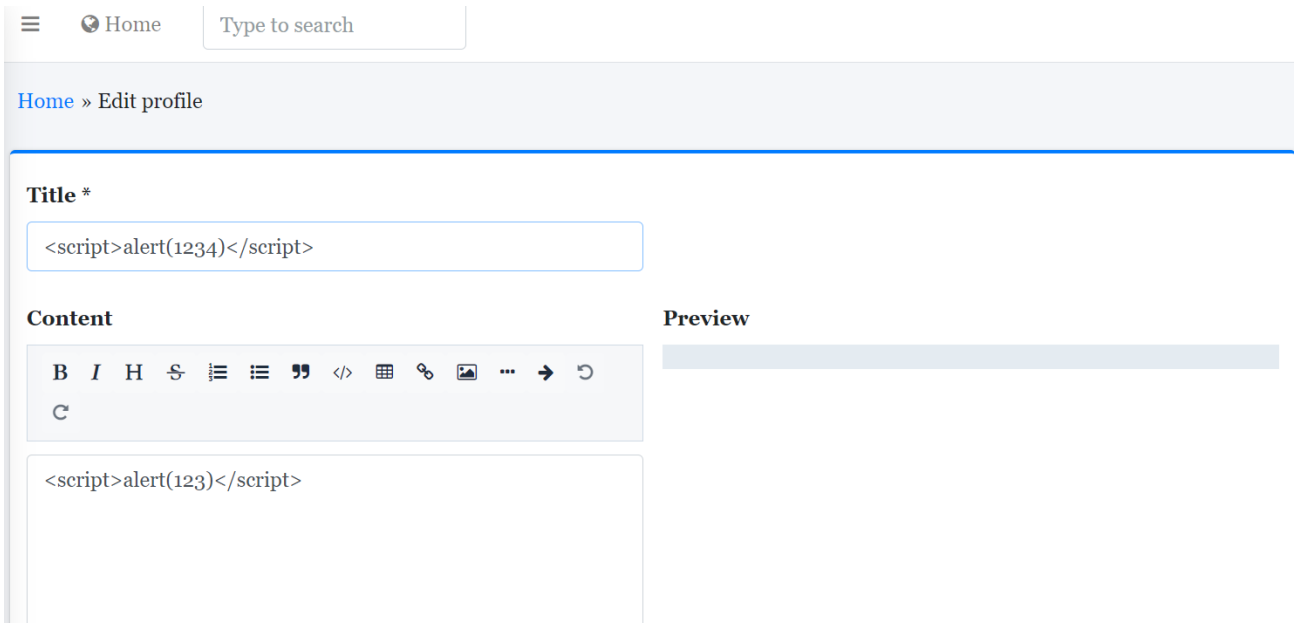
Author

webraybtl@webray.com.cn inc

Proof of Concept

Add payload at the title of edit profile module (click the Save), We can see the alert.


User
My posts
Edit profile
Logout


Home
Type to search
Home » Edit profile
Title *
<script>alert(1234)</script>
Content
Preview
<script>alert(123)</script>


不安全 | 192.168.65.15:8089///author/admin
漏洞平台
漏洞挖掘
192.168.65.15:8089 显示
123
确定