New issue

Jump to bottom

XSS vulnerability in u5cms version 8.3.5 #49

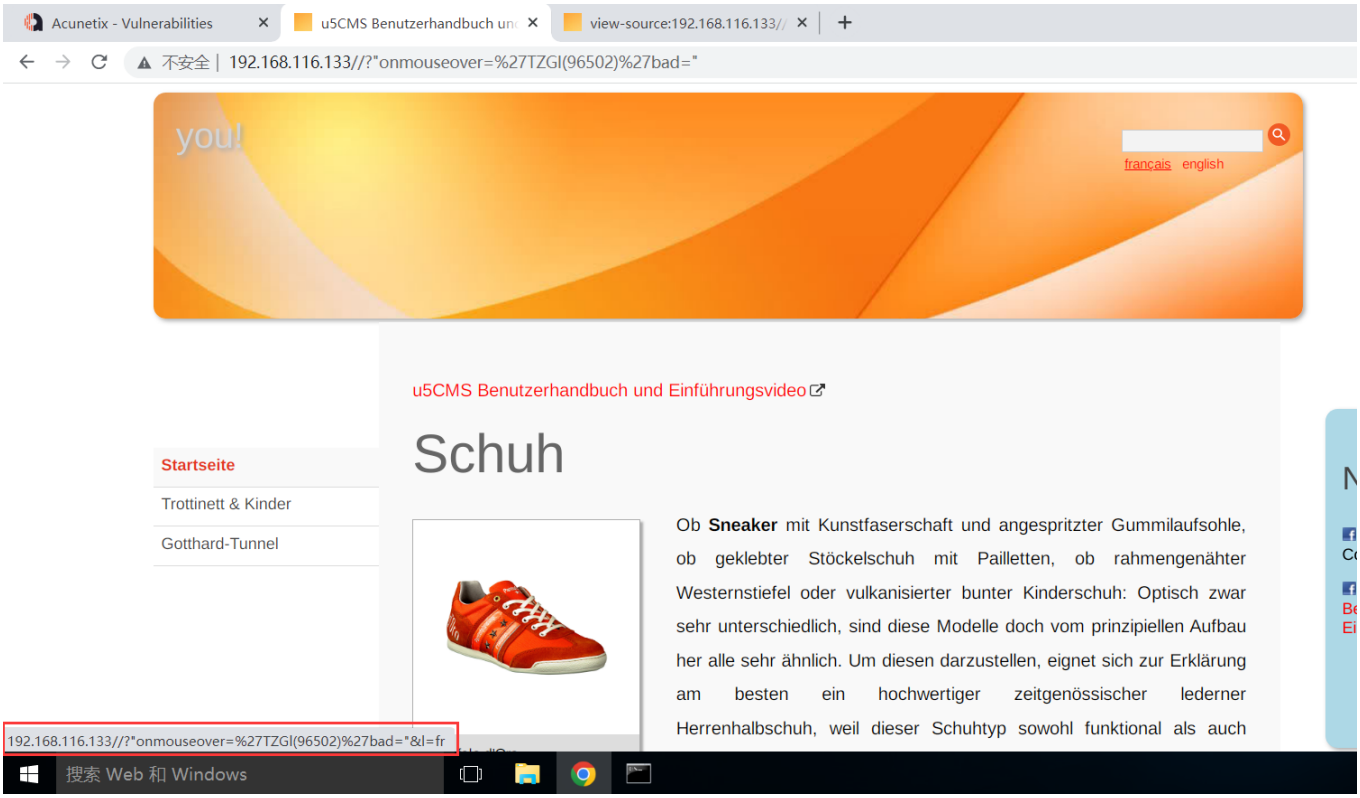
Closed Yu1e opened this issue on Jun 3 · 0 comments

Yu1e commented on Jun 3 • edited

XSS vulnerability in u5cms version 8.3.5

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

When I access the default home page on the web, if the parameter passed in is `/? "Onmouseover=%27tzgl(96502)%27bad="` , it can be found that the passed in parameters appear in the href attribute of a tag in the page.



Then view the source code,you can find the entered parameters and their existence in the href attribute of the a tag

If the parameter passed in is a payload carefully constructed by the attacker, it may cause more serious HTML injection. And if possible, I strongly suggest you check more carefully whether the parameters entered by the user are legal when handling user input and output in the program.

Best wishes!

mrolli mentioned this issue on Aug 20

Sanitize GET parameter q #52

Merged

mrolli closed this as completed on Aug 20

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants