New issue

Jump to bottom

stored XSS #52

Closed **b1nslashsh** opened this issue on Dec 1, 2020 · 2 comments

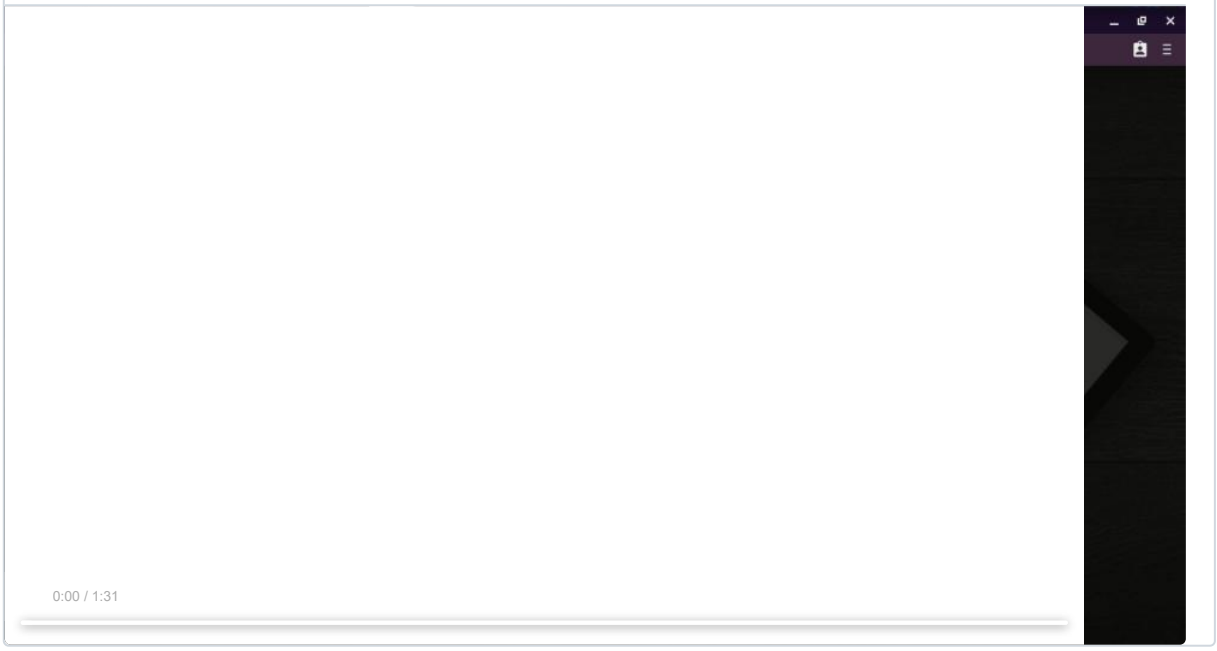
b1nslashsh commented on Dec 1, 2020 • edited

Stored XSS
there is a stored XSS , which is critical because an unauth user can send js code to admin panel , which cloud lead to admin Account takeover.

To Reproduce
Steps to reproduce the behavior:

1. got to s-cart store while adding product to the cart , intercept it and usei the payload in `form_attr` parm

ee.mp4



2. after proceeding the purchase , the code will execute while trying to edit it in the admin panel
   here is the POC video : https://drive.google.com/file/d/1E7AE7EFPTiiEEj8jAKvVAumWKu4PRs0L/view?usp=sharing
   payload used = `"><script>alert("test")</script>`

👍 1

lanhktc referenced this issue in s-cart/core on Dec 1, 2020

Escape data for front-end f4b2811

lanhktc commented on Dec 1, 2020 Collaborator

@b1nslashsh Fixed in s-cart/core@ `f4b2811`
Thank so much!

👍 1 🎉 1

b1nslashsh commented on Dec 1, 2020 • edited Author

@lanhktc Amazing 😍

Also try to give the email in profile so security vulnerability's can share directly without publishing it public
So it reduces the risk
Cheers 🍻,
Muhaimin

👍 1

lanhktc closed this as completed on Dec 5, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants