New issue

Stored & Reflected Cross-Site-Scripting (XSS) in Multiple Locations #1329

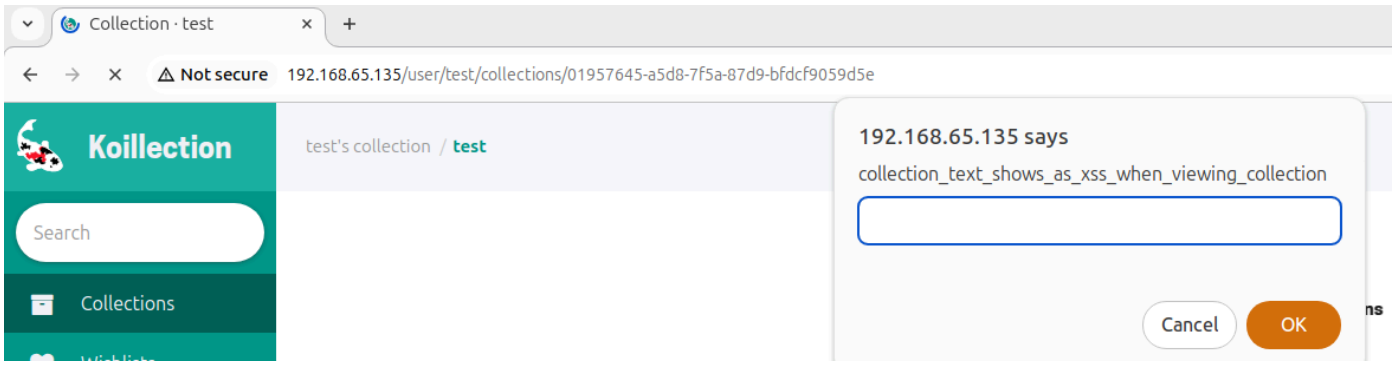
Closed

rt1252 opened on Mar 9 · edited by rt1252 Edits

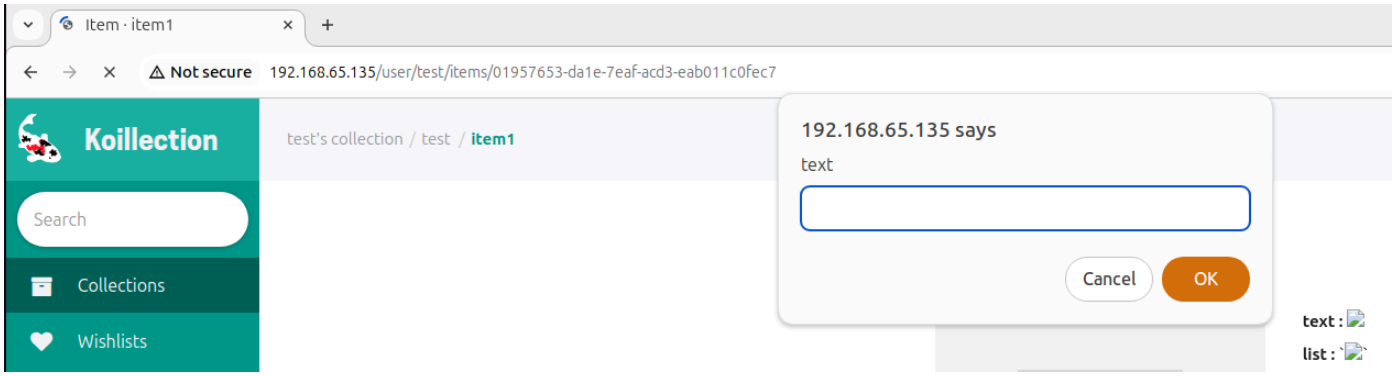
In the Koillection app **@unklerunkle** and I have found stored (persistent) cross site scripting (XSS) in collections, wishlists, and albums.

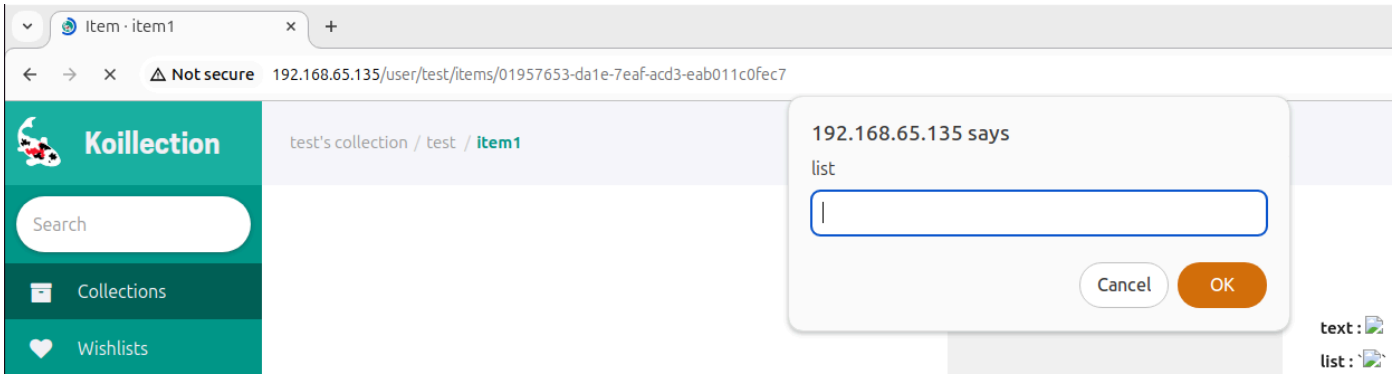
The injectable XSS locations are numbered below, the common payload used to test these locations is `<img src=x onerror=prompt("text")>`
When the numbered locations below are accessed by the author or other user via shared link the stored XSS will appear.

1. [Stored XSS] When creating or editing a collection the text field is vulnerable to stored XSS using the payload above.

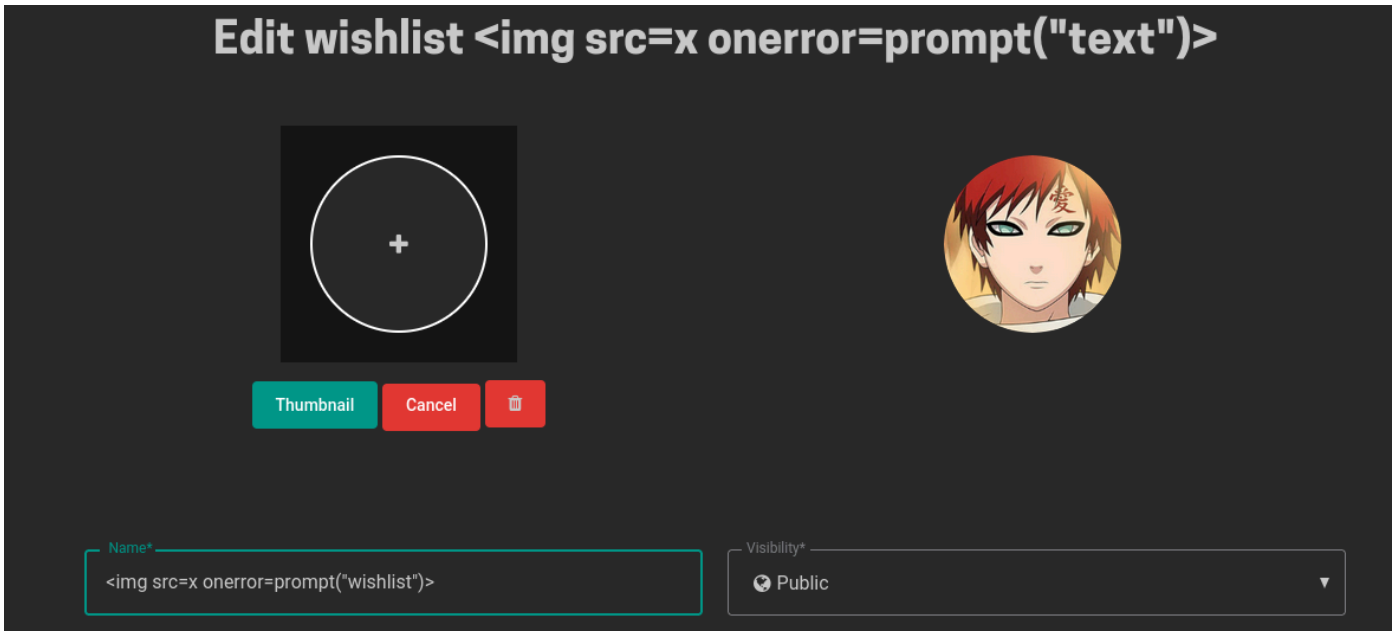


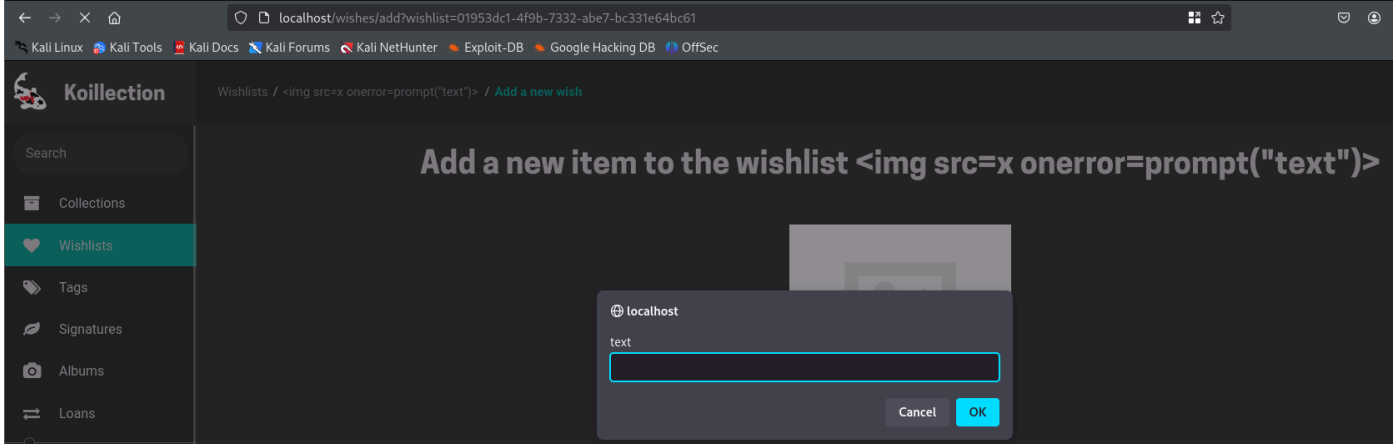
2. [Stored XSS] When creating or editing an item to a collection there are two fields vulnerable to stored XSS: text & list elements. Note to maintainers the long text appropriately sanitizes the input.

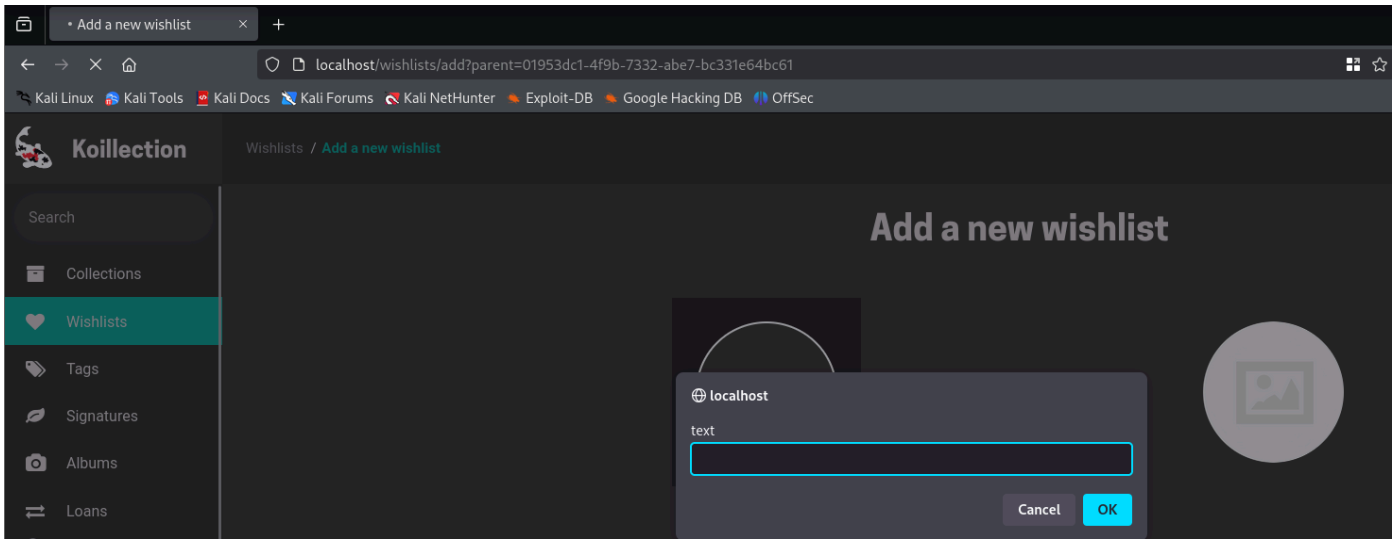




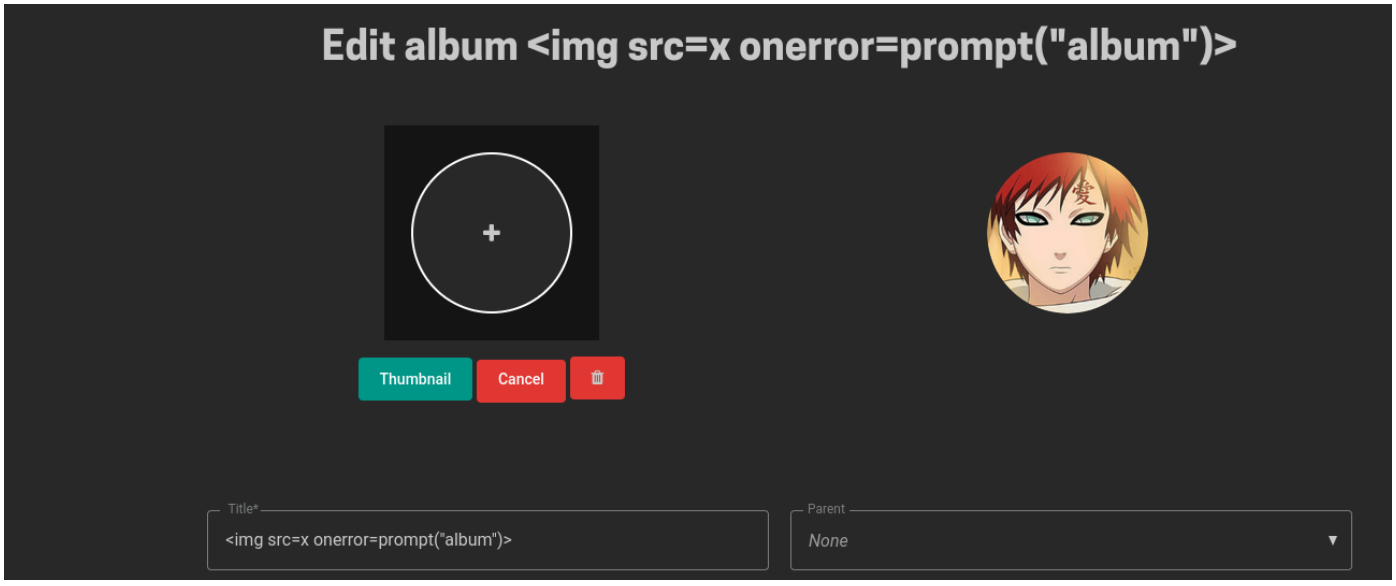
3. [Reflected XSS] Either via creating or editing a wishlist XSS is triggered when adding a new wish or wishlist. This XSS location cannot be accessed by other users as the trigger action of adding a new wish or wishlist can only be accessed by the author.

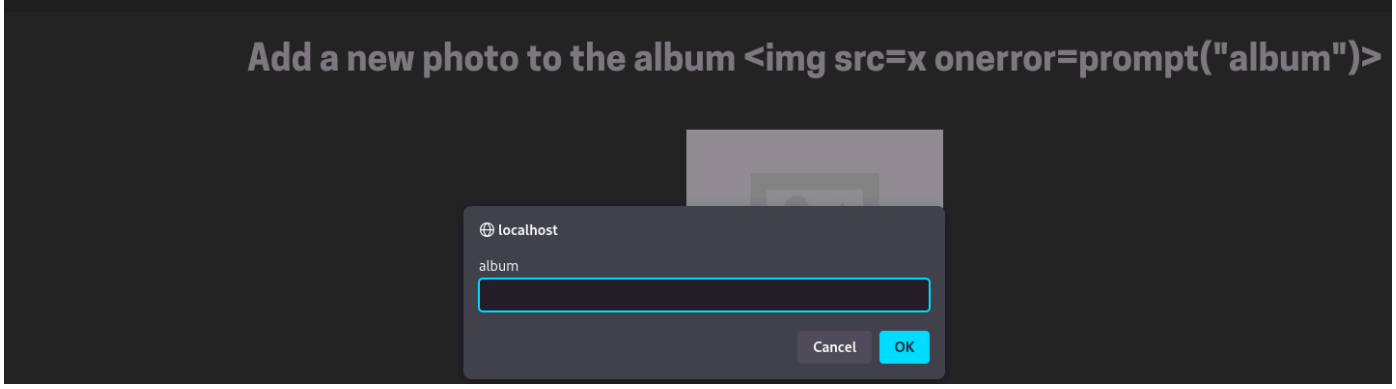


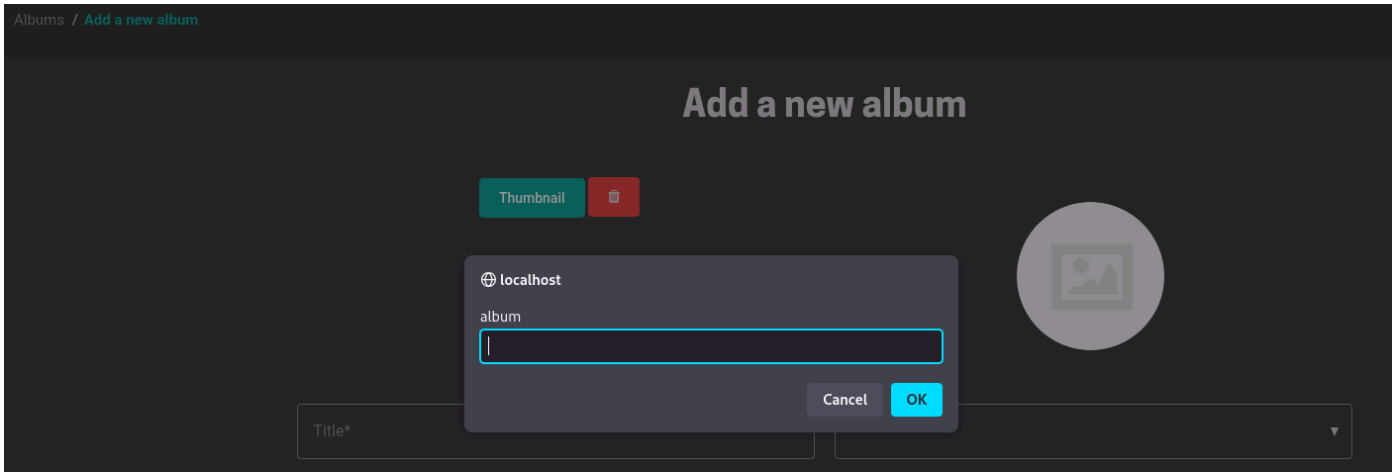




4. [Reflected XSS] Either via creating or editing an album XSS is triggered when adding a new photo or album. This XSS location cannot be accessed by other users as the trigger action of adding a new photo or album can only be accessed by the author.







Impact: Account takeover is usually exploited via XSS cookie theft, luckily this is not possible as session.cookie does have httponly enabled. Redirection to a phishing python remote server via redirect in stored XSS using a window.location payload is possible. While unlikely to be successful as an attack vector it is best to fix these security issues quickly as to protect data integrity.

Remediation: Filter input on arrival and encode data on output. See more https://portswigger.net/web-security/cross-site-scripting/preventing.

Note to maintainers: **@unklerunkle** and I do plan on creating a CVE for this issue in the future.

benjaminjonard on Mar 9 Owner •••

Hello, thanks for reporting this. I just pushed fixes for all reported problems + a few more (when tagging items).

I'll publish a new release tomorrow.

rt1252 on Mar 9 · edited by rt1252 Edits Author •••

Thank you for the quick response, please let us know when the update is pushed and we will retest the issue to confirm it has been remediated.

rt1252 on Mar 11 Author

@unklerunkle and I were able to retest the application and can confirm that update 1.6.11 fixes the XSS issues that we found. Thank you for the quick update **@benjaminjonard**.

rt1252 closed this as completed on Mar 11

benjaminjonard mentioned this last week

[FR] Formatted text field #1023

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with Copilot Agent Mode

No branches or pull requests

Participants