

milesmcc / shynet Public[Code](#) [Issues](#) 53 [Pull requests](#) 9 [Actions](#) [Projects](#) [Security and quality](#)

# Fix stored XSS in urldisplay and iconify template filters #344

Merged milesmcc merged 1 commit into `master` from `claude/fix-xss-analytics-HAVim` [Copy link](#)  
3 weeks ago

[Conversation](#) 0 [Commits](#) 1 [Checks](#) 3 [Files changed](#) 1



milesmcc commented [3 weeks ago](#)

Owner

## Summary

Fixes an unauthenticated stored XSS vulnerability in the dashboard. Attacker-controlled `location` and `referrer` values submitted via the public ingress endpoint were rendered into HTML attributes without escaping, allowing JavaScript execution in the admin's session.

## Root cause

`urldisplay` ([helpers.py:193](#)) — interpolated the raw URL into single-quoted `href='{url}'` and `title='{url}'` attributes. A payload like `http://x' onfocus='...' autofocus='` passed the `startswith("http")` check, then closed the `href` attribute early and injected new attributes.

`iconify` ([helpers.py:184](#)) — called by `urldisplay` with the same tainted input. `urlparse().netloc` preserves quote characters, and the netloc was inserted raw into a double-quoted `src="..."` attribute.



## Fix

Apply `escape()` to the three unescaped interpolation points. This matches the existing `escape(display_url)` pattern already present on the same line. Django's `escape()` converts `'` → `&#x27;` and `"` → `&quot;`, preventing attribute break-out in both contexts.

## Affected pages

- `/dashboard/service/<uuid>/` (location and referrer tables)
- `/dashboard/service/<uuid>/locations/`

  [Fix stored XSS in urldisplay and iconify template filters](#) ... ✓ [2d02f48](#)

  **milesdcc** merged commit **2298546** into `master` [3 weeks ago](#) View details  
2 of 3 checks passed

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

**Reviewers**

No reviews

**Assignees**

No one assigned

**Labels**

None yet

**Projects**

None yet

**Milestone**

No milestone

**Development**

Successfully merging this pull request may close these issues.

None yet

**2 participants**

