methosiea / **xenforo-2-xss** Public

Code Issues Pull requests Actions Projects Security and quality Insights

main 1 Branch 0 Tags Go to file Code

methosiea 2.x	394f8dd · last month	
.gitignore	initial commit	2 months ago
README.md	2.x	last month
xss.html	initial commit	2 months ago
xss.sh	initial commit	2 months ago

README

XenForo 2.x - Stored XSS via Placeholder Collision

Stored Cross-Site Scripting vulnerability in XenForo's structured text mention rendering (`XF\Str\Formatter::linkStructuredTextMentions()`).

Root Cause

Placeholder collision between `autoLinkStructuredText()` and `linkStructuredTextMentions()` during OUTPUT rendering. When a mention username contains `\x1A` bytes matching placeholder patterns, `removeHtmlPlaceholders()` strips them, and `restorePlaceholders()` later restores raw HTML inside a `data-username` attribute — breaking attribute context and enabling XSS.

Attack Chain

1. `autoLinkStructuredText()` converts URLs to `<a>` tags, stored as `\x1A{id}\x1A` placeholders
2. Crafted username in `@[id:username]` contains placeholder-matching `\x1A` bytes
3. `removeHtmlPlaceholders()` strips the placeholder from the username
4. `htmlspecialchars()` escapes the remaining username into `data-username`

5. `restorePlaceholders()` restores the `<a>` tag **inside** the attribute — XSS

Three bypass techniques combine to get the payload past input filters:

- **URL encoding** — `%1A` passes `cleanString()`, decoded to `\x1A` during output via `urldecode()`
- **Invalid BBCode** — `[x=` prevents the StructuredText filter from processing nested mentions
- **Nested mentions** — only the outer `@[id:...]` is converted; the inner one survives to output rendering

Files

- `xss.sh` — automated PoC that authenticates, posts the payload, and generates a report
- `xss.html` — rendered HTML test report

Usage

```
# Edit xss.sh to set FORUM_URL, ADMIN_USERNAME, ADMIN_PASSWORD, TARGET_USER_ID
./xss.sh
# Open xss.html to view the report
```

Requirements

- Authenticated XenForo account with posting privileges
- XenForo <= 2.3.7+ (works in older/newer versions of XenForo 2.x with slight adjustments)

Contributors 1

methosiea metho

Languages

Shell 70.7% **HTML** 29.3%