fix: HTML-escape all user data in slide generator to prevent stored XSS #274

Open TemaDeveloper wants to merge 1 commit into `nextlevelbuilder:main` from `TemaDeveloper:fix/slide-generator…`

TemaDeveloper commented last week

Summary

Fixes the **Stored XSS vulnerability** (CVSS 8.1) in `generate-slide.py` reported in #247.

- **HTML-escape all 46 `data.get()` calls** across all 7 slide generator functions using `html.escape()` — prevents `<script>`, `<img onerror>`, and `<iframe>` injection into generated HTML
- **Add URL scheme validation** for `cta_url` in the CTA slide — blocks `javascript:` URI injection by only allowing `http://`, `https://`, `#`, and `/` schemes
- **Escape the deck `<title>`** in the template rendering to prevent metadata injection
- **Cast bar chart `value` to `int()`** in the style attribute to prevent CSS injection via the `height` property

Approach

Added two small helpers at the top of the file:

- `_e(value, default)` — wraps `html.escape(str(...))` for all content injection points
- `_safe_url(url, default)` — validates URL scheme before escaping for `href` attributes

Testing

Verified with the exact PoC payload from #247:

- `<script>alert('XSS')</script>` in title → rendered as escaped text
- `<img src=x onerror=alert(1)>` in badge → rendered as escaped text
- `javascript:alert(document.domain)` in cta_url → replaced with `#`

- Normal slide content (demo deck) renders identically — no regressions

Closes #247

`fix: HTML-escape all user data in slide generator to prevent XSS` ··· `396e9dd`

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.

Slide Generator Multiple Stored XSS

1 participant