& Maniphest > T266508 Create Task

☑ PolINY: Stored XSS (CVE-2020-29003)

☑ Closed, Resolved ☑ Public SECURITY

Actions

-

Assigned To

ashley

Authored By

ashley 2020-10-26 20:43:57 (UTC+0)





a PollNY (Backlog)

→ Social-Tools (PolINY)

Referenced Files

F32416835: new-stored-xss-2020-10-27 21:19:33 (UTC+0)

F32415006: PollNY-Stored-XSS-2020-10-26 20:48:48 (UTC+0)

Aklapper

ashley

Bawolff

Isarra

Icawte Legoktm

sbassett

Description

Like **T266400** but only for PolINY this time around...

Prerequisites: social tools setup (MW 1.34 with SocialProfile, and for this particular bug, also need PolINY)

- 1. Create a poll via Special:CreatePoll, or edit an existing one via Special:UpdatePoll
- 2. Have an answer option contain something like <script>alert('XSS')</script>
- $\textbf{4. When viewing the poll's page in the } ~ \texttt{NS_POLL} ~ name space, the malicious code gets executed despite that it damn well shouldn't also be a substitution of the malicious code gets of the substitution of the malicious code gets of the malicious code gets$

The last step is also true for polls embedded on other wiki pages via the pollembed parser tag.

Details

Project Subject

P mediawiki/extensions/PollNY [SECURITY] Fix stored XSS via poll choices on Poll: pages etc.

P mediawiki/extensions/PollNY [SECURITY] Fix stored XSS via poll choices on Poll: pages etc.

Customize query in gerrit

Related Objects

Mentions

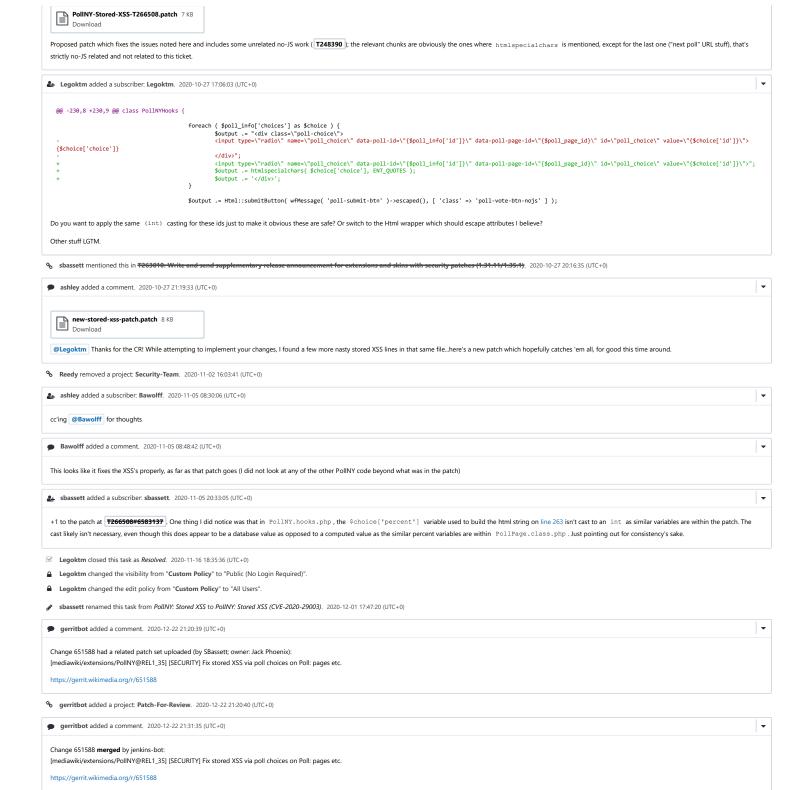
Mentioned In

Mentioned Here T248390: Better NoJS support

ashley created this task. 2020-10-26 20:43:57 (UTC+0)

- Restricted Application added a subscriber: Aklapper. · View Herald Transcript 2020-10-26 20:43:58 (UTC+0)
- ashley claimed this task. 2020-10-26 20:44:26 (UTC+0)
- % ashley added projects: Vuln-XSS, PolINY.
- % Restricted Application added a project: **Social-Tools**. · View Herald Transcript 2020-10-26 20:44:27 (UTC+0)
- ashley updated the task description. (Show Details) 2020-10-26 20:45:54 (UTC+0)

ashley moved this task from Backlog to PolINY on the Social-Tools board. 2020-10-26 20:48:01 (UTC+0)



% Maintenance_bot removed a project: Patch-For-Review. 2020-12-22 22:10:28 (UTC+0)