RandomGameUnit: Stored XSS (CVE-2020-27957)

Closed, Resolved   Public   SECURITY

Actions

Assigned To

ashley

Authored By

ashley
2020-10-25 10:42:30 (UTC+0)

Tags

Security
RandomGameUnit (Backlog)
Vuln-XSS
Social-Tools (RandomGameUnit)

Referenced Files

F32412979: xss.patch
2020-10-25 10:45:07 (UTC+0)

Subscribers

Aklapper

ashley

Isarra

Icawte

Legoktm

Description

Prerequisites: social tools setup (MW 1.34 with SocialProfile, and for this particular bug, also need PictureGame, PollNY, QuizGame and RandomGameUnit)

1. Create a game (for example, a picture game via `Special:PictureGameHome` ; but the bug also happens with PollNY polls and QuizGame quizzes since RandomGameUnit fails to properly escape titles/options for all three types of games)
2. Have its title contain something like `<script>alert('XSS')</script>`
3. Save the game to ensure that it's created (obviously!)
4. When using RandomGameUnit, whether directly via adding the parser tag to a wiki page or as a more "fixed" part of the UI (e.g. in the Nimbus skin), note how the malicious code gets executed despite that it damn well shouldn't

This is somewhat of a continuation of the fixes done in **fde2cd7a5e9b675e6c78003f47e21bd8634271f9** for PictureGame's own creation/editing form.

Details

Project	Subject
mediawiki/extensions/RandomGameUnit	[SECURITY] Run stored, user-generated input from DB through htmlspecialchars() to avoid stored XSS originating from PictureGame/PollNY/QuizGame data
mediawiki/extensions/RandomGameUnit	[SECURITY] Run stored, user-generated input from DB through htmlspecialchars() to avoid stored XSS originating from PictureGame/PollNY/QuizGame data
mediawiki/extensions/RandomGameUnit	[SECURITY] Run stored, user-generated input from DB through htmlspecialchars() to avoid stored XSS originating from PictureGame/PollNY/QuizGame data
mediawiki/extensions/RandomGameUnit	[SECURITY] Run stored, user-generated input from DB through htmlspecialchars() to avoid stored XSS originating from PictureGame/PollNY/QuizGame data

Customize query in gerrit

Related Objects

Mentions

Mentioned In

rERGUb6a3dff8287d: [SECURITY] Run stored, user-generated input from DB through htmlspecialchars()...
rERGU47d7729a63e5: [SECURITY] Run stored, user-generated input from DB through htmlspecialchars()...
rERGU2ff6abc3052d: [SECURITY] Run stored, user-generated input from DB through htmlspecialchars()...
~~T266508: PollNY: Stored XSS (CVE-2020-29003)~~
~~T263810: Write and send supplementary release announcement for extensions and skins with security patches (1.31.11/1.35.1)~~
rERGU69bcc1ae9f82: [SECURITY] Run stored, user-generated input from DB through htmlspecialchars()...

Mentioned Here

rEPGAfde2cd7a5e9b: [SECURITY] Fix some obvious XSS holes

ashley created this task. 2020-10-25 10:42:30 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2020-10-25 10:42:32 (UTC+0)

ashley claimed this task. 2020-10-25 10:43:19 (UTC+0)

ashley added projects: **RandomGameUnit**, **Vuln-XSS**.

Restricted Application added a project: **Social-Tools**. · View Herald Transcript 2020-10-25 10:43:20 (UTC+0)

ashley added a comment. 2020-10-25 10:45:07 (UTC+0)

xss.patch 2 KB
Download

Proposed and tested patch which adds relevant, missing `htmlspecialchars()` calls to all three callback functions to ensure that whatever is stored in the DB is properly sanitized before being sent back.

ashley moved this task from **Backlog** to **RandomGameUnit** on the **Social-Tools** board. 2020-10-25 10:45:34 (UTC+0)

ashley mentioned this in **rERGU69bcc1ae9f82: [SECURITY] Run stored, user-generated input from DB through htmlspecialchars()....** 2020-10-26 04:21:20 (UTC+0)

ashley closed this task as *Resolved*. 2020-10-26 04:23:00 (UTC+0)

ashley added a subscriber: **Legoktm**.

A slightly modified patch, with input from @Legoktm , was submitted and merged as 69bcc1ae9f8246f59b626d72348e11bd2ddb2231, which fixes this issue.

Legoktm changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2020-10-26 04:31:59 (UTC+0)

Legoktm changed the edit policy from "**Custom Policy**" to "All Users".

Reedy removed a project: **Security-Team**. 2020-10-26 04:35:17 (UTC+0)

sbassett mentioned this in ~~**T263810: Write and send supplementary release announcement for extensions and skins with security patches (1.31.11/1.35.1)**~~. 2020-10-26 17:05:36 (UTC+0)

gerritbot added a comment. 2020-10-26 19:38:49 (UTC+0)

Change 636484 had a related patch set uploaded (by SBassett; owner: SBassett):
[mediawiki/extensions/RandomGameUnit@REL1_35] [SECURITY] Run stored, user-generated input from DB through htmlspecialchars() to avoid stored XSS originating from PictureGame/PollNY/QuizGame data

https://gerrit.wikimedia.org/r/636484

gerritbot added a project: **Patch-For-Review**. 2020-10-26 19:38:49 (UTC+0)

gerritbot added a comment. 2020-10-26 19:48:51 (UTC+0)

Change 636488 had a related patch set uploaded (by SBassett; owner: SBassett):
[mediawiki/extensions/RandomGameUnit@REL1_34] [SECURITY] Run stored, user-generated input from DB through htmlspecialchars() to avoid stored XSS originating from PictureGame/PollNY/QuizGame data

https://gerrit.wikimedia.org/r/636488

gerritbot added a comment. 2020-10-26 19:53:51 (UTC+0)

Change 636489 had a related patch set uploaded (by SBassett; owner: SBassett):
[mediawiki/extensions/RandomGameUnit@REL1_31] [SECURITY] Run stored, user-generated input from DB through htmlspecialchars() to avoid stored XSS originating from PictureGame/PollNY/QuizGame data

https://gerrit.wikimedia.org/r/636489

ashley mentioned this in ~~**T266508: PollNY: Stored XSS (CVE-2020-29003)**~~. 2020-10-26 20:43:57 (UTC+0)

sbassett renamed this task from *RandomGameUnit: Stored XSS* to *RandomGameUnit: Stored XSS (CVE-2020-27957)*. 2020-10-28 19:35:11 (UTC+0)

gerritbot added a comment. 2020-10-28 19:39:22 (UTC+0)

Change 636489 **merged** by jenkins-bot:
[mediawiki/extensions/RandomGameUnit@REL1_31] [SECURITY] Run stored, user-generated input from DB through htmlspecialchars() to avoid stored XSS originating from PictureGame/PollNY/QuizGame data

https://gerrit.wikimedia.org/r/636489

sbassett mentioned this in **rERGU2ff6abc3052d: [SECURITY] Run stored, user-generated input from DB through htmlspecialchars()....** 2020-10-28 19:43:47 (UTC+0)

gerritbot added a comment. 2020-12-22 21:36:40 (UTC+0)

Change 636488 **merged** by Umherirrender:
[mediawiki/extensions/RandomGameUnit@REL1_34] [SECURITY] Run stored, user-generated input from DB through htmlspecialchars() to avoid stored XSS originating from PictureGame/PollNY/QuizGame data

https://gerrit.wikimedia.org/r/636488

gerritbot added a comment. 2020-12-22 21:39:33 (UTC+0)

Change 636484 **merged** by Umherirrender:
[mediawiki/extensions/RandomGameUnit@REL1_35] [SECURITY] Run stored, user-generated input from DB through htmlspecialchars() to avoid stored XSS originating from PictureGame/PollNY/QuizGame data

https://gerrit.wikimedia.org/r/636484

sbassett mentioned this in **rERGU47d7729a63e5: [SECURITY] Run stored, user-generated input from DB through htmlspecialchars()....** 2020-12-22 21:54:46 (UTC+0)

sbassett mentioned this in **rERGUb6a3dff8287d: [SECURITY] Run stored, user-generated input from DB through htmlspecialchars()....**

Maintenance_bot removed a project: **Patch-For-Review**. 2020-12-22 22:10:44 (UTC+0)