

I. Information

searchReplace A simple search and replace plugin. Licensed under the [GPL](#)
[Deactivate](#) Version 1.2.2 | By Joost Berculo | [View details](#)

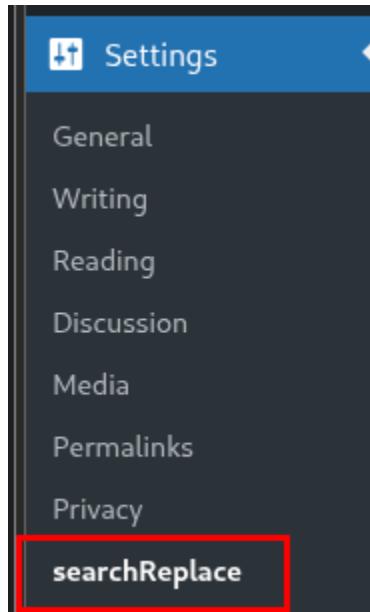
- Plugin: searchReplace
- Version: 1.2.2
- Author: Joost Berculo
- Vulnerability: Stored XSS
- Description: The vulnerability exists in the Description user-controlled input field, which is stored in the database and rendered without proper output escaping, leading to a Stored Cross-Site Scripting (XSS) vulnerability.

II. POC

- Payload: <h1>Test <script>alert("XSS Hacked")</script></h1>
- Vulnerable Location: **Add new searchReplace**
- Vulnerable Field: **Description** (user-controlled input field)

Step 1: Access the plugin settings page

- Log in to WordPress as an **Administrator**
- Navigate to the plugin configuration page:



- Main interface

searchReplace	Regular Expression	Type	Options
BBcode bold [b]	Yes	Only comments	delete edit
BBcode italic [i]	Yes	Only comments	delete edit
BBcode blockquote [q]	Yes	Only comments	delete edit
BBcode underline [u]	Yes	Only comments	delete edit
BBcode strikethrough [s]	Yes	Only comments	delete edit
BBcode text color [color]	Yes	Only comments	delete edit
BBcode image [img]	Yes	Only comments	delete edit
BBcode size [size]	Yes	Only comments	delete edit
BBcode font [font]	Yes	Only comments	delete edit
BBcode code [code]	Yes	Only comments	delete edit
BBcode blockquote 2 [quote]	Yes	Only comments	delete edit
BBcode ordered list 1 [list=1]	Yes	Only comments	delete edit
BBcode ordered list 1 [list=re1]	Yes	Only comments	delete edit
BBcode list item [*]	Yes	Only comments	delete edit
BBcode background color [bg]	Yes	Only comments	delete edit
BBcode simple url replace [url]	Yes	Only comments	delete edit
BBcode advanced url replace [url] (with link name)	Yes	Only comments	delete edit
Youtube [youtube]youtube_id[/youtube] (425x350)	Yes	Only posts and pages	delete edit
Test	Yes	Disabled	delete edit

Add new searchReplace

Description:

Search for:

Replace by:

- Add new searchReplace, In the **Description** field, enter the following payload: <h1>Test<script>alert("XSS Hacked")</script></h1>

Add new searchReplace

Description:

Search for:

Replace by:

Replace type:

Is regular expression

- Click “Add new searchReplace” or Reload, after reloading the page, the injected JavaScript payload is executed and an XSS popup is displayed.

The screenshot shows a web browser window with the URL `127.0.0.1:8080/wp-admin/options-general.php?page=searchReplace.php`. A modal dialog box is displayed, containing the text "127.0.0.1:8080 says XSS Hacked". An "OK" button is visible at the bottom right of the dialog. The background page shows a table titled "searchReplace Options Updated" with various configuration items. The "Tools" menu item in the sidebar is highlighted.

- The screenshot shows the stored XSS payload rendered in the DOM, as observed in the browser's Developer Tools (Elements tab).

The screenshot shows the browser's developer tools with the "Elements" tab selected. In the main pane, there is a table with two rows. The second row, which has a red box around it, contains a script tag that has been injected into the DOM. The script tag contains the code `<script>alert("XSS Hacked")</script>`. The "Settings" menu item in the sidebar is highlighted.

