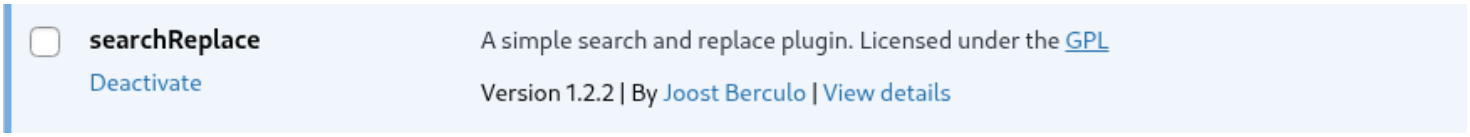
I. Information



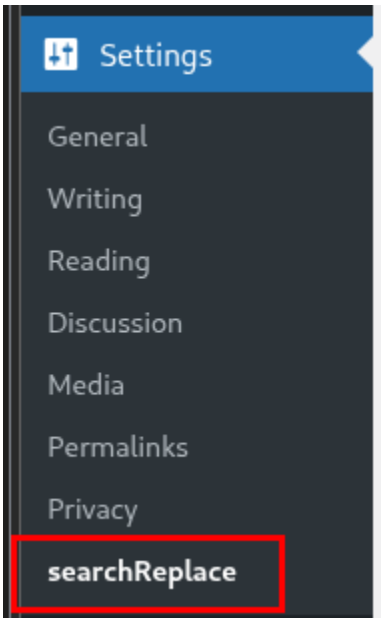
- Plugin: searchReplace
- Version: 1.2.2
- Author: Joost Berculo
- Vulnerability: Stored XSS
- Description: The vulnerability exists in the Description user-controlled input field, which is stored in the database and rendered without proper output escaping, leading to a Stored Cross-Site Scripting (XSS)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

II. POC

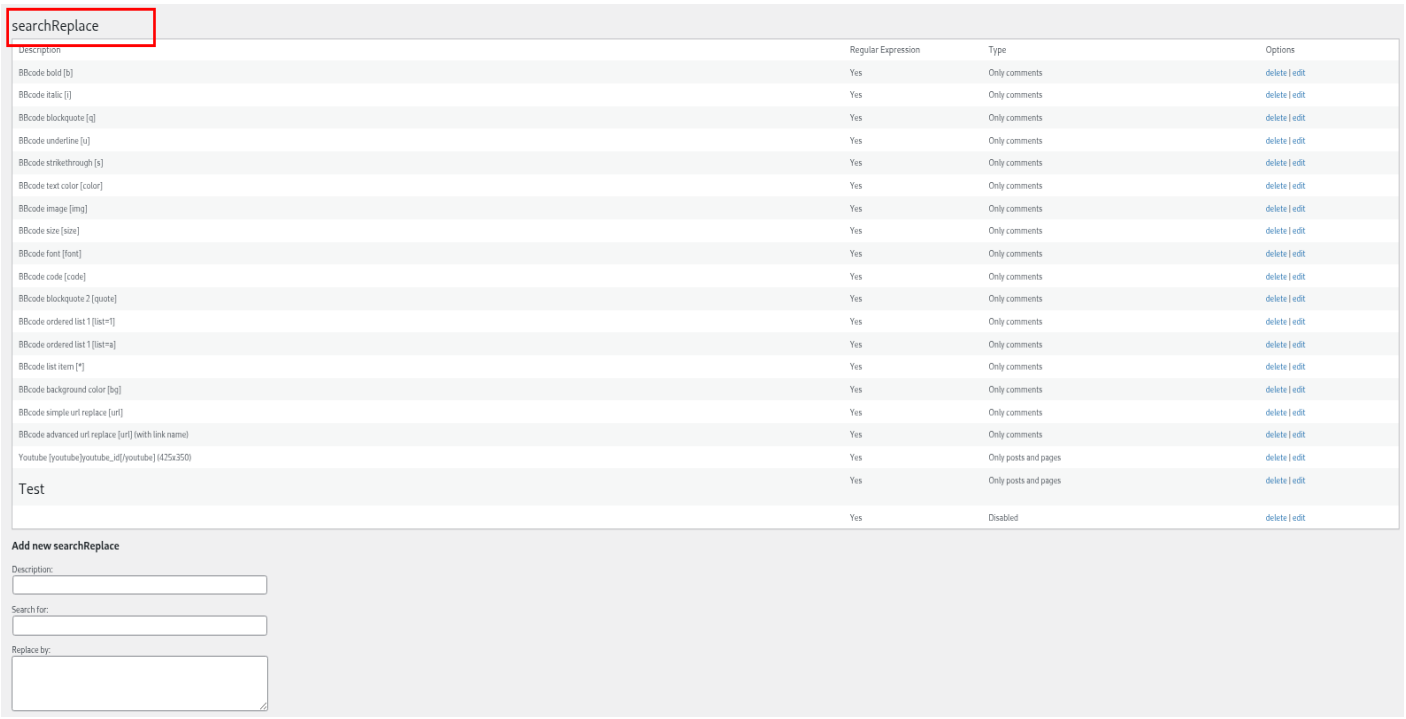
- Payload: <h1>Test <script>alert("XSS Hacked")</script></h1>
- Vulnerable Location: **Add new searchReplace**
- Vulnerable Field: **Description** (user-controlled input field)

Step 1: Access the plugin settings page

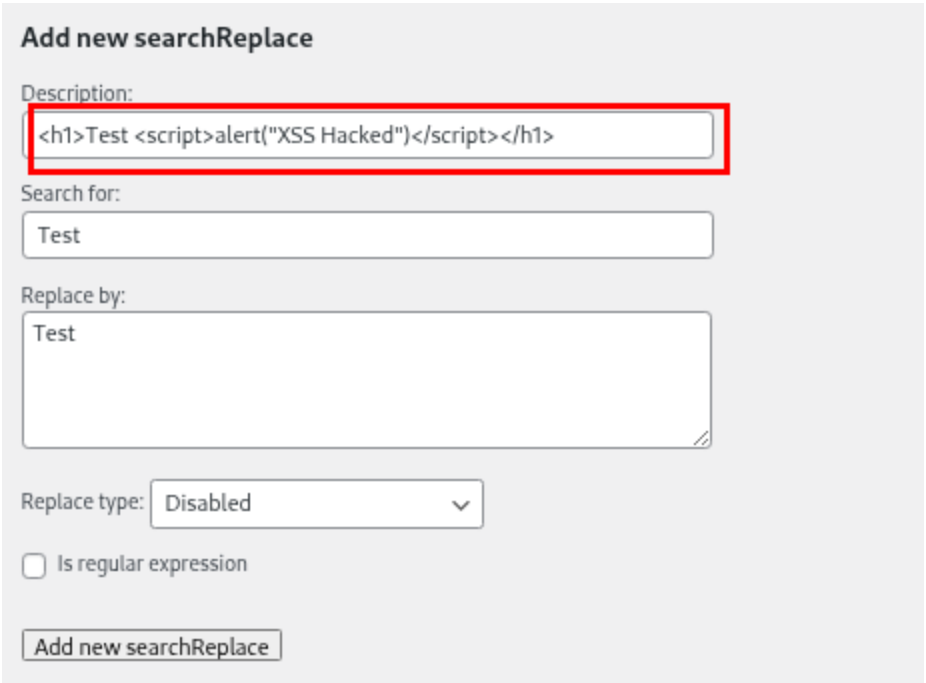
- Log in to WordPress as an **Administrator**
- Navigate to the plugin configuration page:



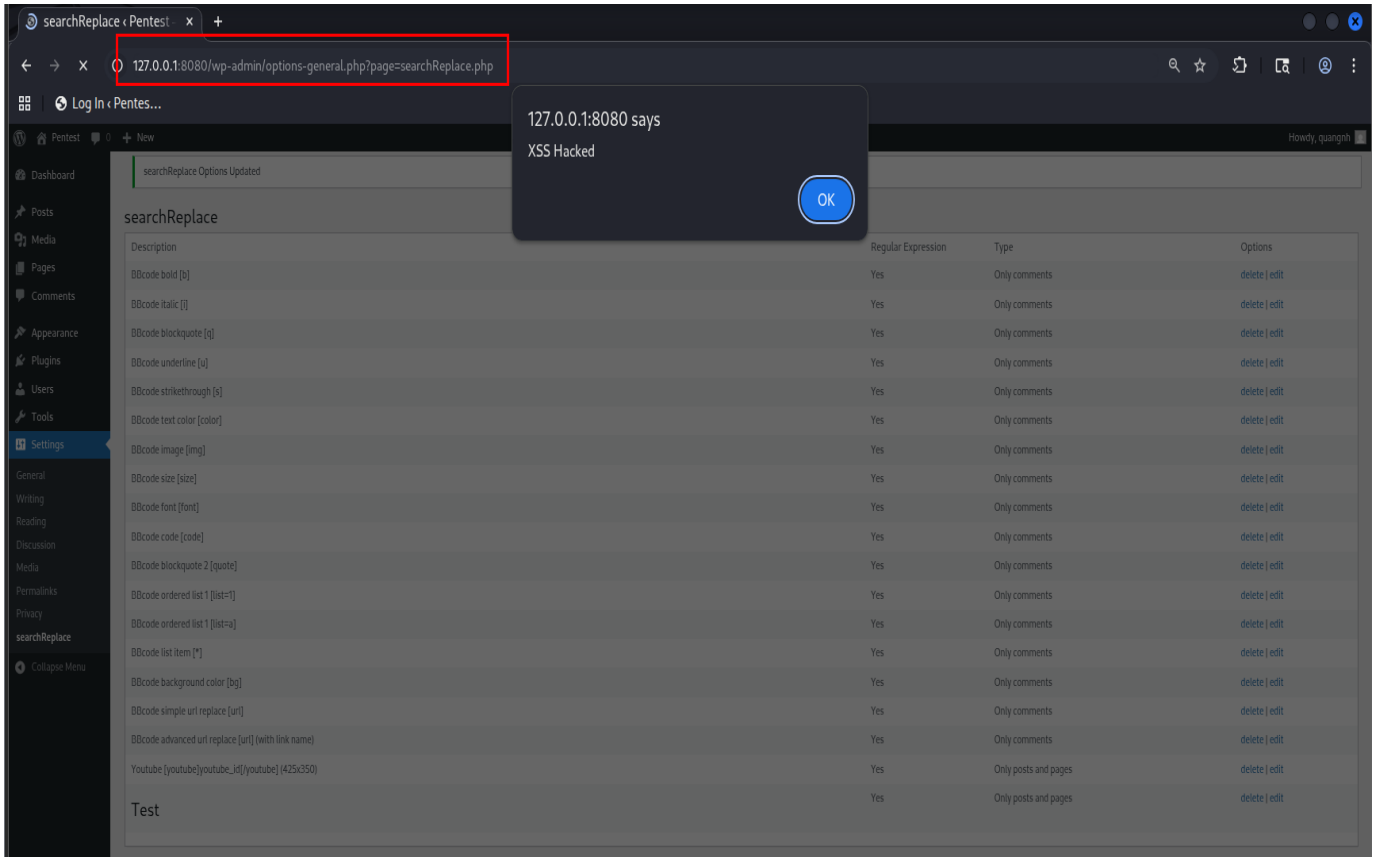
- Main interface



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



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