Vulnerability Name: Stored XSS

Product Name: Wonder CMS

Product URL: https://www.wondercms.com/

Version No: 3.5.0

Description:

WonderCMS is vulnerable to stored cross-site scripting (XSS) via the “Website Title” field in the admin dashboard. An authenticated low-privileged admin can inject malicious JavaScript which executes every time a user visits the homepage. This occurs due to a lack of proper input sanitization and output encoding when rendering the title in the site layout.

Impact:

This vulnerability allows attackers to persistently inject JavaScript that executes in the context of any site visitor's browser, leading to session hijacking, redirection to phishing pages, or potential lateral movement in admin panels. As no CSP (Content Security Policy) is enforced, the attack surface remains broad.

CWE:

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Steps to Reproduce:

1. Deploy WonderCMS locally or access a hosted instance.
2. Login as admin.
3. Navigate to “Settings” → “Website Title”.
4. Input the following payload: <script>alert(document.domain)</script>
5. Save settings and view the home page.
6. The script will execute immediately.

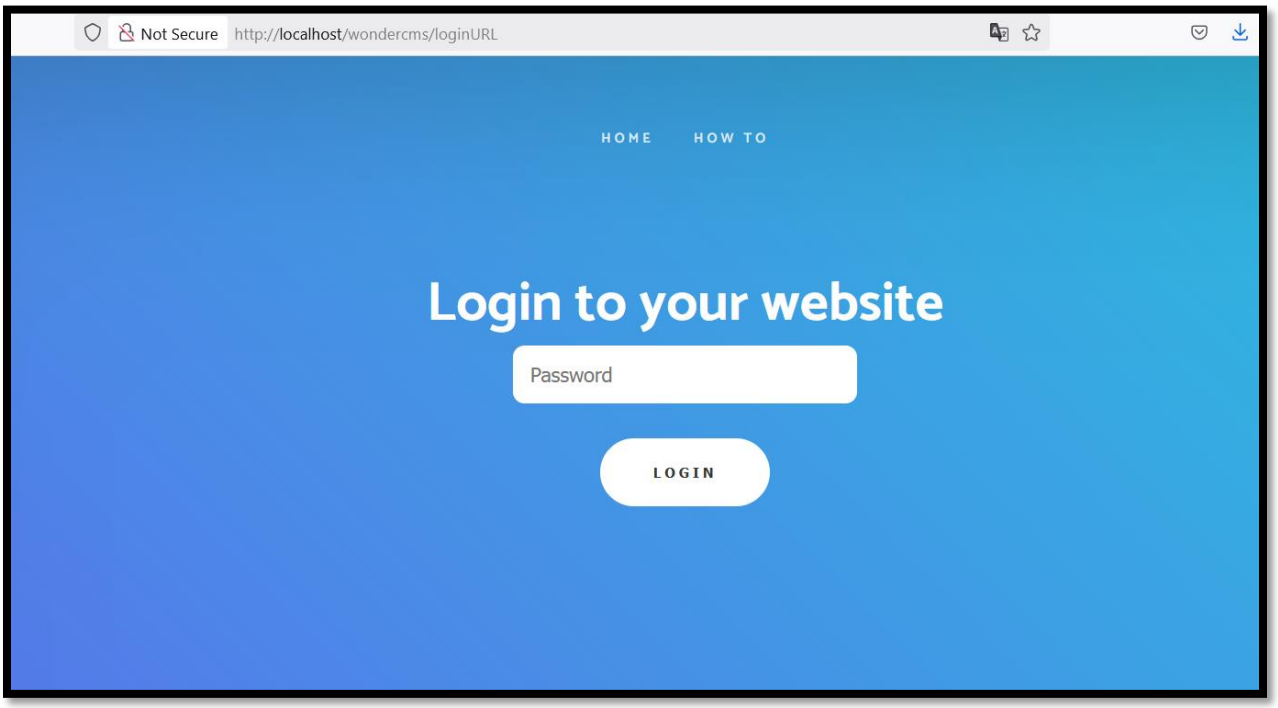
Recommendation:

The input for the Website Title and all user-supplied fields should be sanitized for special characters and encoded properly before rendering. It is also recommended to implement a strict Content Security Policy (CSP) to prevent inline script execution and to escape any dynamic output using context-aware escaping.

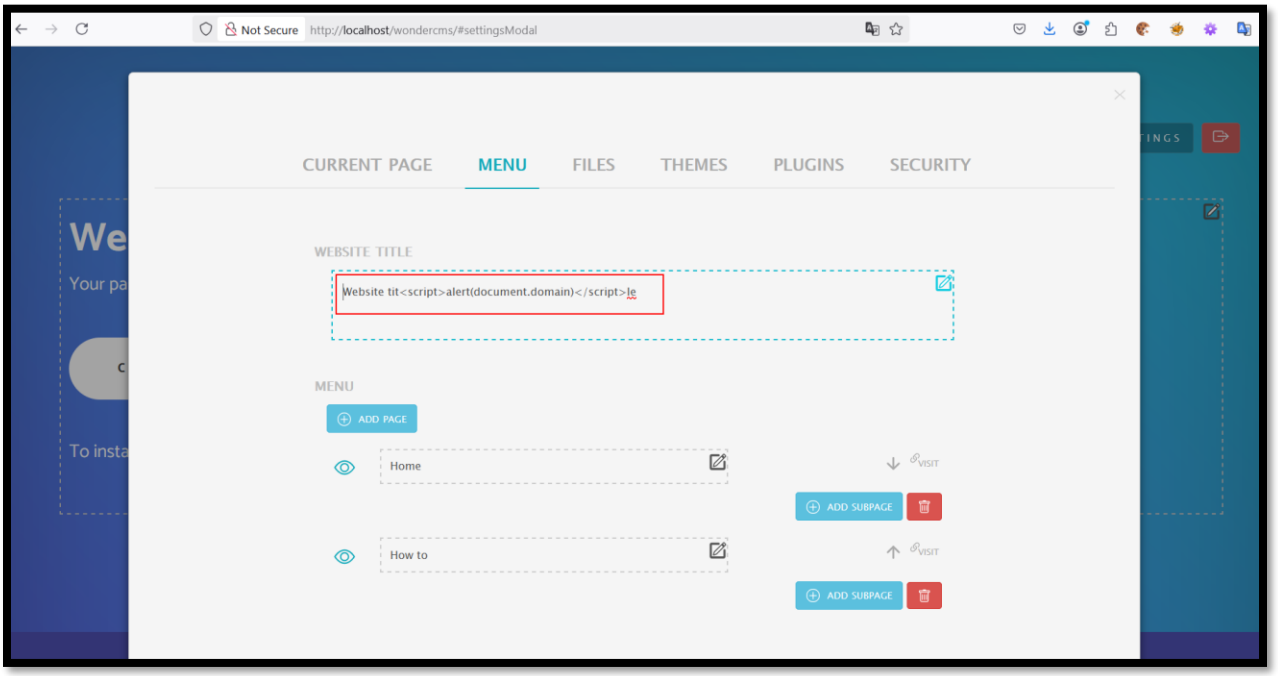
Reference:

https://gist.github.com/aashiqahamedn/4c3540d8a7de32fc8bc2b253a70f6338

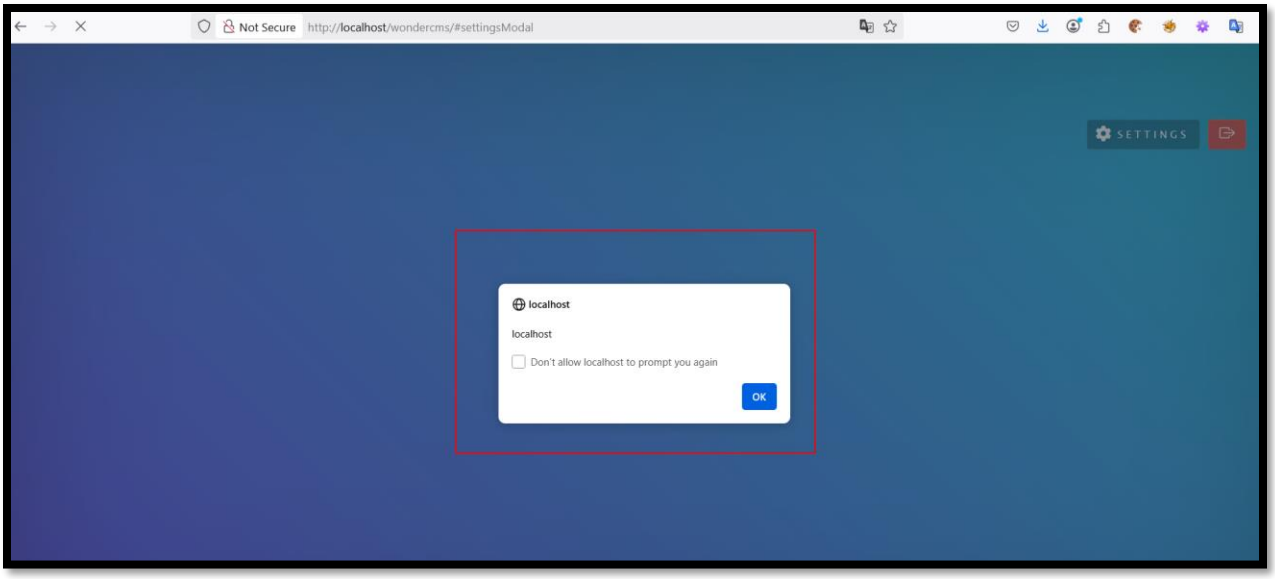
POC:


Not Secure
http://localhost/wondercms/loginURL
HOME
HOW TO
Login to your website
Password
LOGIN

(a)


Not Secure
http://localhost/wondercms/#settingsModal
CURRENT PAGE
MENU
FILES
THEMES
PLUGINS
SECURITY
WEBSITE TITLE
Website tit<script>alert(document.domain)</script>le
MENU
ADD PAGE
Home
ADD SUBPAGE
How to
ADD SUBPAGE

(b)


Not Secure
http://localhost/wondercms/#settingsModal
SETTINGS
localhost
localhost
Don't allow localhost to prompt you again
OK

(c)