⑂ main ▾   ···

word-press / Simple Job Board—Stored Cross-Site Scripting - 2.md

🐯 BigTiger2020 Update Simple Job Board—Stored Cross-Site Scripting - 2.md   ⟳ History

👥 1 contributor

☰ 14 lines (14 sloc) │ 969 Bytes   ···

Exploit Title: WordPress Plugin Simple Job Board——Stored Cross-Site Scripting

Exploit Author: Thinkland Security Team

Date: 16/09/2021

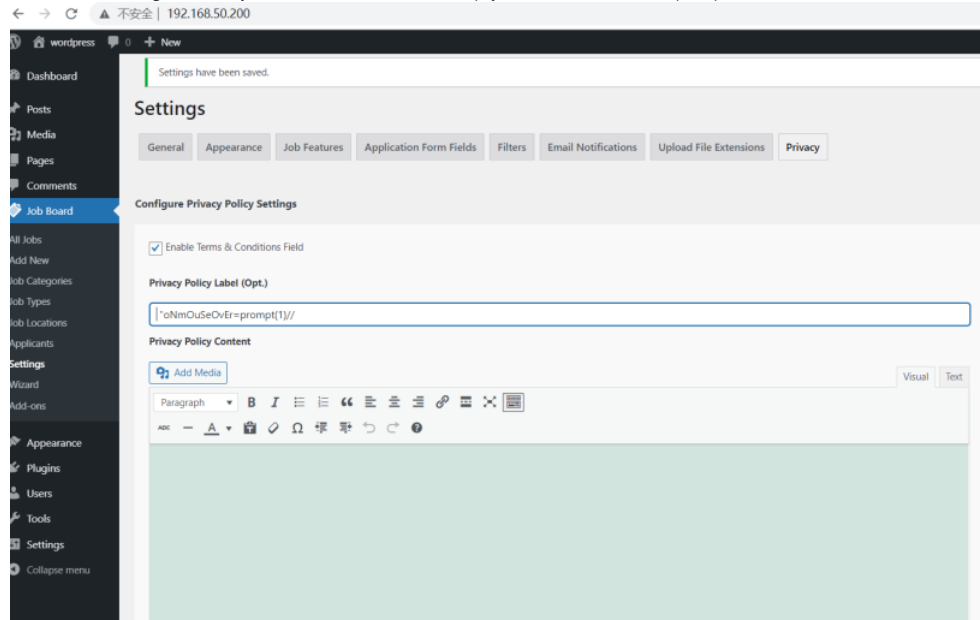# Vendor Homepage: https://wordpress.org/plugins/simple-job-board/

Version : V 2.9.4
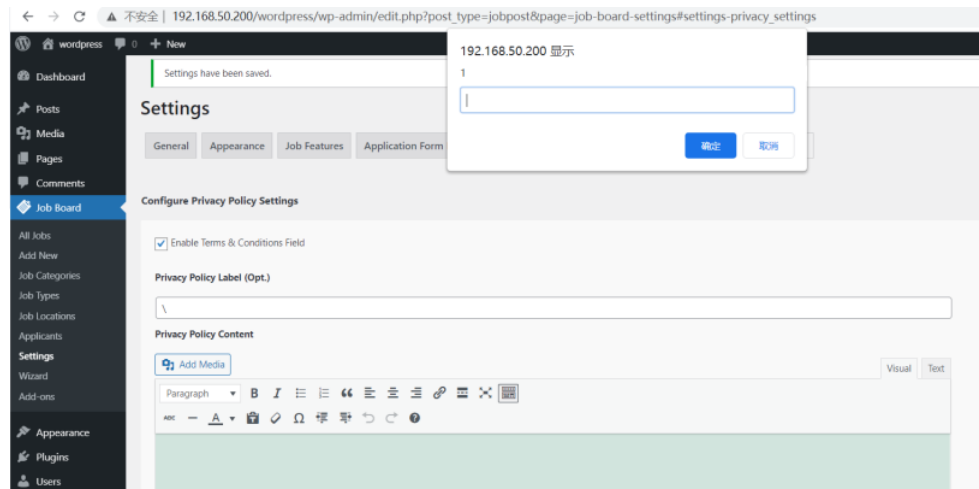
Vulnerability Type: Stored Cross-Site Scripting

Tested on Windows 10 、 XAMPP

Vulnerability proof：

1. Job Board >> Settings >> Privacy >> Add title and enter the XSS payload： "OnMoUsEoVeR=prompt(1)//

2. Click Save Changes,You will observe that the payload successfully got stored into the database and when you are triggering the same functionality at that time JavaScript payload is executing successfully and we are getting a pop-up.

3.Vulnerability proof: