

main

...

word-press / WpGenius Job Listing.md



BigTiger2020 Update WpGenius Job Listing.md

History

1 contributor

11 lines (11 sloc) | 787 Bytes

...

## Exploit Title: WrodPress Plugin WpGenius Job Listing ——"Settings" Stored Cross-Site Scripting

Exploit Author: Thinkland Security Team

Vendor Homepage: <https://wordpress.org/plugins/wpgenious-job-listing/>

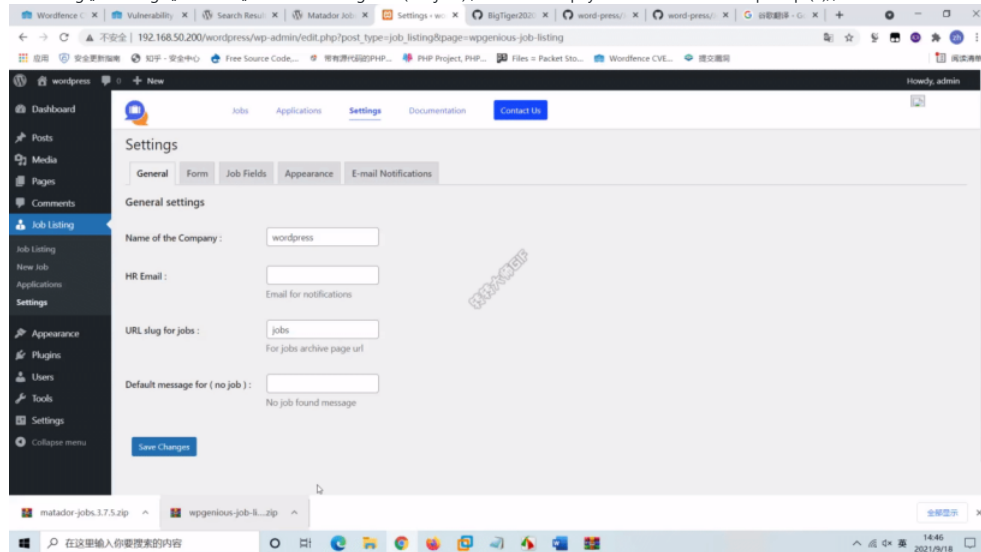
Version : V 1.0.2

Vulnerability Type: Stored Cross-Site Scripting

Tested on Windows 10 、XAMPP

Vulnerability proof:

1. Job Listing » Settings » General » Default message for ( no job ) ,insert the xss payload "OnMoUsEoVeR=prompt(1)("//



2. Job Listing » Settings » E-mail notifications » Reply-To and Subject,insert the xss payload "OnMoUsEoVeR=prompt(1)("//

