

Advertisement



betterscan-ce (<https://github.com/marcinguy/betterscan-ce>)

Code Scanning/SAST/Static Analysis/Linting using many tools/Scanners with One Report (Code, IaC) -
Betterscan Community Edition (CE)

Python ☆ 336 🍴 55

Edit  (edit.html?id=38893) Report  (mailto:info@topcodersonline.com)

Our sensors found this exploit at: <https://cxsecurity.com/ascii/WLB-2022080005> (<https://cxsecurity.com/ascii/WLB-2022080005>)

Below is a copy:

```
# Exploit Title: WordPress Plugin WP-UserOnline 2.87.6 - Stored Cross-Site Scripting (XSS)
# Date: 21/07/2022
# Exploit Author: Steffin Stanly
# Vendor Homepage: https://github.com/lesterchan/wp-useronline
# Software Link: https://wordpress.org/plugins/wp-useronline/
# Version: <=2.87.6
# Tested on Windows
```

How to reproduce vulnerability:

1. Install WordPress 6.0.1
2. Install and activate WP-UserOnline plugin.
3. Navigate to Setting >> WP-UserOnline and enter the data into the User(s) Browsing Site.
4. Add the following payload "><script>alert(1)</script>" and save changes
5. On visiting the dashboard, You will observe that the payload successfully got stored in the database and when you are triggering the same functionality in that time JavaScript payload is executing successfully and we are getting a pop-up.

Copyright ©2022 Exploitalert.

All trademarks used are properties of their respective owners. By visiting this website you agree to Terms of Use (terms-of-use.html).

We collect and process your personal information for the following purposes: **Analytics, Security**. Learn more

OK Decline