

Posts

CVE-2020-23761 Stored XSS vulnerability in subrion CMS Version <= 4.2.1

🕒 April 9, 2021 👤 [admin \(http://hidden-one.co.in/author/admin/\)](http://hidden-one.co.in/author/admin/) 💬 [Leave a comment \(http://hidden-one.co.in/2021/04/09/cve-2020-23761-stored-xss-vulnerability-in-subrion-cms-version/#respond\)](http://hidden-one.co.in/2021/04/09/cve-2020-23761-stored-xss-vulnerability-in-subrion-cms-version/#respond)

- 1) install subrion CMS version (4.2.1)
- 2) login into admin account
- 3) go to Financial tab and click on transactions
- 4) Select “add transaction” button and inject xss payload on the “payment gateway” column and save the entry
- 5) now come to the admin dashboard and you will see the XSS popping

← [CVE-2020-15020 Stored XSS on Elementor WordPress plugin \(http://hidden-one.co.in/2020/07/07/cve-2020-1020-stored-xss-on-elementor-wordpress-plugin/\)](http://hidden-one.co.in/2020/07/07/cve-2020-1020-stored-xss-on-elementor-wordpress-plugin/)

[CVE-2020-23762 Stored XSS vulnerability in the Larsens Calender plugin Version <= 1.2 for WordPress → \(http://hidden-one.co.in/2021/04/09/cve-2020-23762-stored-xss-vulnerability-in-the-larsens-calender-plugin-version/\)](http://hidden-one.co.in/2021/04/09/cve-2020-23762-stored-xss-vulnerability-in-the-larsens-calender-plugin-version/)

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

COMMENT

NAME *

EMAIL *

WEBSITE

☐ SAVE MY NAME, EMAIL, AND WEBSITE IN THIS BROWSER FOR THE NEXT TIME I COMMENT.

POST COMMENT

Search ...

RECENT POSTS

[CVE-2020-23763 SQL injection leading to Authentication bypass in "Online Book Store 1.0" \(http://hidden-one.co.in/2021/04/09/cve-2020-23763-sql-injection-leading-to-authentication-bypass-in-online-book-store-1-0/\)](http://hidden-one.co.in/2021/04/09/cve-2020-23763-sql-injection-leading-to-authentication-bypass-in-online-book-store-1-0/)

[CVE-2020-23762 Stored XSS vulnerability in the Larsens Calender plugin Version <= 1.2 for WordPress \(http://hidden-one.co.in/2021/04/09/cve-2020-23762-stored-xss-vulnerability-in-the-larsens-calender-plugin-version/\)](http://hidden-one.co.in/2021/04/09/cve-2020-23762-stored-xss-vulnerability-in-the-larsens-calender-plugin-version/)

[CVE-2020-23761 Stored XSS vulnerability in subrion CMS Version <= 4.2.1 \(http://hidden-one.co.in/2021/04/09/cve-2020-23761-stored-xss-vulnerability-in-subrion-cms-version/\)](http://hidden-one.co.in/2021/04/09/cve-2020-23761-stored-xss-vulnerability-in-subrion-cms-version/)

[CVE-2020-15020 Stored XSS on Elementor WordPress plugin \(http://hidden-one.co.in/2020/07/07/cve-2020-1020-stored-xss-on-elementor-wordpress-plugin/\)](http://hidden-one.co.in/2020/07/07/cve-2020-1020-stored-xss-on-elementor-wordpress-plugin/)

[CVE-2020-13888 Kordil EDMS through 2.2.60rc3 allows stored XSS \(http://hidden-one.co.in/2020/06/17/cve-2020-13888-kordil-edms-through-2-2-60rc3-allows-stored-xss/\)](http://hidden-one.co.in/2020/06/17/cve-2020-13888-kordil-edms-through-2-2-60rc3-allows-stored-xss/)

 ([HTTPS://NEWS.YCOMBINATOR.COM/RSS](https://news.ycombinator.com/rss)) [HACKER NEWS \(HTTPS://NEWS.YCOMBINATOR.COM/\)](https://news.ycombinator.com/)

[Spacekaren.sucks \(https://spacekaren.sucks/\)](https://spacekaren.sucks)

[Emacs User Survey – 2022 Results \(https://emacs-survey.org/results/3425413930\)](https://emacs-survey.org/results/3425413930)

[Twitter's anti-Mastodon filter evasion \(https://infosec.exchange/@postmodern/109523637731779949\)](https://infosec.exchange/@postmodern/109523637731779949)

[Next, Nest, Nuxt Nust? \(https://www.twilio.com/blog/comparing-nextjs-nestjs-nuxt-gatsby\)](https://www.twilio.com/blog/comparing-nextjs-nestjs-nuxt-gatsby)

[EsPiFF: An ESP32 in the Raspberry Pi form factor \(https://github.com/MDCService/EsPiFF\)](https://github.com/MDCService/EsPiFF)

[Show HN: I made an Ethernet transceiver from logic gates \(https://imihaiojov.tk/blog/posts/eth-to-spi/\)](https://imihaiojov.tk/blog/posts/eth-to-spi/)

[Programming with Unicon \[pdf\] \(http://unicon.org/book/ub-nightly.pdf\)](http://unicon.org/book/ub-nightly.pdf)

[America's social and political turmoil during the 1910s and 20s \(https://quilllette.com/2022/12/17/americas-forgotten-crisis/\)](https://quilllette.com/2022/12/17/americas-forgotten-crisis/)

[Let's Encrypt now supports ACME-CAA: closing the DV loophole \(https://www.devever.net/~hl/acme-caa-live\)](https://www.devever.net/~hl/acme-caa-live)

[Quite OK Image is now my favorite asset format \(https://nullprogram.com/blog/2022/12/18/\)](https://nullprogram.com/blog/2022/12/18/)