

The only thing you have to do is to make someone with the permissions to create users opening the malicious page, while connected. At the end you will have a new admin user, ready to be used to login without nobody knowing it. @support I'm not skilled enough to figure out how to solve, but maybe a token could help to protect the session (considering that it cannot be put in the malicious form)? Yes, in this case, we need admin have session cookie click the link. 66 Re: CSRF vulnerability on Rukovoditel 2.8.3 Hacker can add new user with admin privilege ■ 11 Mar 2021, 21:21 Again you are tesing with localhost and Xampp. By default session are the same for all localhost folders that is why you can send request form html form if there is logged users in http://localhost//rukovoditel_2.8.3/ But in live server you can't do it. TuongNC 66 Re: CSRF vulnerability on Rukovoditel 2.8.3 Hacker can add new user with admin privilege 66 support wrote: 1 Again you are tesing with localhost and Xampp. By default session are the same for all localhost folders that is why you can send request form html form if there is logged users in http://localhost//rukovoditel_2.8.3/ But in live server you can't do it. In live server, I just need ADMIN click to my link and go to my website, method POST will be trigger. 0 support Site Admin 66 Re: CSRF vulnerability on Rukovoditel 2.8.3 Hacker can add new user with admin privilege ■ 11 Mar 2021, 21:57 You can't do any action if you are not logged. So any html files like this will redirect to login. 0 TuongNC 66 Re: CSRF vulnerability on Rukovoditel 2.8.3 Hacker can add new user with admin privilege ■ 11 Mar 2021, 22:08 Yes, if user has been logged in? marajah 66 Re: CSRF vulnerability on Rukovoditel 2.8.3 Hacker can add new user with admin privilege ■ 12 Mar 2021, 00:50 66 support wrote: ↑ You can't do any action if you are not logged. So any html files like this will redirect to login. It's not the attacker that needs to be logged, but the victim. When the victim is logged and click on the page, the actions will be done on behalf of the victim https://en.wikipedia.org/wiki/Cross-sit ... st_forger There are some public database of the exploits of this and other types that could be directed to Rukovoditel. Probably they are not crazily dangerous, but I'm not skilled enough to say https://packetstormsecurity.com/search/?q=rukovoditel https://www.exploit-db.com/ https://www.cvedetails.com/product/5413 ... r_id=19833 ۵ TuongNC 66 Re: CSRF vulnerability on Rukovoditel 2.8.3 Hacker can add new user with admin privilege ■ 12 Mar 2021, 07:40 66 marajah wrote: ↑ 66 support wrote: 1 You can't do any action if you are not logged. So any html files like this will redirect to login. It's not the attacker that needs to be logged, but the victim. When the victim is logged and click on the page, the actions will be done on behalf of the victim https://en.wikipedia.org/wiki/Cross-sit ... st_forger There are some public database of the exploits of this and other types that could be directed to Rukovoditel. Probably they are not crazily dangerous, but I'm not skilled enough to say https://packetstormsecurity.com/search/?q=rukovoditel https://www.exploit-db.com/ https://www.cvedetails.com/product/5413 ... r_id=19833 Nice comment <3 66

Re: CSRF vulnerability on Rukovoditel 2.8.3 Hacker can add new user with admin privilege

13 Mar 2021, 03:44

This looks like a critical security bug requiring an immediate patch. Typical basic CSRF vulnerability.

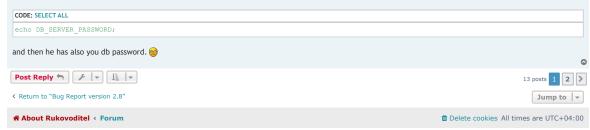
It does not matter that attacker is not logged in, the problem is that attacker can easily achieve that the script is activated by a logged-in user, e.g. by sending the admin a link to a malicious page by e-mail. If the admin clicks the link, the attacker has succeeded.

Even worse is that it seems to me (I have not tested it) that Rukovoditel is not protected against CSFRs at all. If so, any available actions could be activated by an attacker using this technique, everything you can imagine. Adding new entries, adding new fields, deleting entities, changing admin's email and password ... countless options.

@TuongNC Did you have a chance to tests other forms in the app?

@support Please fix this asap. Also, please confirm that there are measures against CSFR in the Rukovoditel and there are no other forms with this vulnerability.

Edit: Vulnerability is real, I just successfully reproduced this. No need for the same domain, it works even if the code is somewhere else. Malicious script on localhost hacked my rukovoditel 2.8.3 running on professional webhosting with SSL. With this, the attacker will gain access to the admin's account. Then he can simply create field type PHPFormula in any entity, input code



Powered by phpBB® Forum Software © phpBB Limited Privacy | Terms