

Forum:[Hack Forums](#)

Thread: [Need someone to verify CSRF](#)

0xB9 - November 14, 2018, 11:41 am

As title says... I found a CSRF but owner of the CMS is saying it's not a vuln, just need someone to take a minute to confirm.

It seems very obvious by the message he sent me that he's not sure how a CSRF works..

Quote:what I have found is if you do this all while logged in and using the same browser session this worked, and I was able to use the script offline to create a new user. However, if I was logged in using Chrome, and then tried using the offline script in incognito mode (or another browser or even another computer), this DID NOT WORK.

If you have a quick minute and not a total noob PM for info.

connectover - November 15, 2018, 4:29 am

Yeah he seems to think running scripts offline will have an effect on a foreign server? He's batshit.

Abruptum - November 15, 2018, 7:14 am

(Nov 14, 2018 12:41 PM)0xB9 Wrote: [\[CITE\]](#) As title says... I found a CSRF but owner of the CMS is saying it's not a vuln, just need someone to take a minute to confirm I'm not retarded.

It seems very obvious by the message he sent me that he's not sure how a CSRF works..

If you have a quick minute and not a total noob PM for info.

It seems like don't understand the reason why this is a problem. Try to find possible exploitation vectors which will impress him (like creating a new page when he visits your malicious CSRF)

0xB9 - November 15, 2018, 11:28 am

(Nov 15, 2018 08:14 AM)Abruptum Wrote: [\[CITE\]](#) It seems like don't understand the reason why this is a problem. Try to find possible exploitation vectors which will impress him (like creating a new page when he visits your malicious CSRF)

The site uses CSRF tokens, but it fails to verify the token when making a request which leads to the CSRF.

And I have exploited it for him, it allows to create another admin. He even did it himself, but wrote it off since it didn't work on 2 different computers or whatever the hell he tried to do...

(Nov 15, 2018 05:29 AM)connectover Wrote: [\[CITE\]](#) Yeah he seems to think running scripts offline will have an effect on a foreign server? He's batshit.

Yea.. he's trying to exploit a CSRF in 2 different browsers/computers... so no shit it's not working for him. LOL

?Criminal - November 15, 2018, 9:11 pm

Own the site and when he realizes you have DBMS access he will shit him self and get right on it, I would just show you logged into the admin panel a full on root is overkill but you can potentially escalate the csrf2rce