

Forum:[Hack Forums](#)

Thread: [MyBB xss](#)

Icey. - August 12, 2021, 11:27 am

Hello,

Here is a minor xss that has almost no impact but thought i would share it because i'm to lazy to report it.

Code `usercp.php?action=do_editlists&my_post_key=key&manage="{any html}&delete=id`

Problem:

They have not sanitized the output that happens when removing someone from the friendlist.

Here is the code:

<https://github.com/mybb/mybb/blob/e99ec544ef0dbe243c64e6f41c9d4bdac090473d/usercp.php#L3233>

linkinpork - August 12, 2021, 11:56 pm

(Aug 12, 2021 11:27 AM)Icey. Wrote: [\[CITE\]](#) Code

`usercp.php?action=do_editlists&my_post_key=key&manage="{any html}&delete=id`

Problem:

They have not sanitized the output that happens when removing someone from the friendlist.

Hi,

There's a CSRF token required to run the `do_editlists` function, along with the myBB secret token that you use for posts. The myBB secret is static, but cannot be extracted unless you proxied the victim (since it is placed in POST data, not Set-Cookie). The CSRF token is also POST data.

You can argue that this is doable with MITM though, but that beats the point of weaponization.

POC: